Universidad Autónoma de Madrid

Tesis Doctoral

Teoría de números clásica en tres contextos diferentes

Autor:
José Granados Palomo

Tutor:
D. Fernando Chamizo Lorente

Una tesis presentada en cumplimiento de los requisitos para el grado de Doctor en Matemáticas

en el

Departamento de Matemáticas
Facultad de Ciencias

13 de enero de 2020

UAM
Universidad Autónoma de Madrid

ICMAT
INSTITUTO DE CIENCIAS MATEMÁTICAS

Índice

Resumen

La *Teoría de Números* es una disciplina casi inabarcable dentro de las Matemáticas y se ocupa de una infinidad de fenómenos y problemas que surgen al estudiar los diferentes conjuntos numéricos. En este trabajo se presentan tres contextos particulares (distribuidos en tres Capítulos respectivos) donde está presente un contacto sutil de esta disciplina con otras tales como la *Variable Compleja*, el *Análisis de Fourier*, el *Análisis Numérico* o la *Geometría Algebraica*; muestra de la interacción entre diferentes ramas que permite obtener resultados como los que se van a producir.

En el primer Capítulo se analizará el fenómeno de la distribución del espectro de autovalores del Operador de Laplace-Beltrami (llamada Ley de Weyl) cuando se define sobre los grupos de Lie clásicos considerados como variedades Riemannianas, a las cuales se les puede aplicar la *Teoría de Operadores*. Aunque el punto de partida es un resultado ya existente sobre dicha distribución, la localización de un error en una desigualdad llevará a reformular la prueba en términos de una herramienta propia de la *Teoría de Números* como son las formas modulares. Gracias a esta herramienta y a otros resultados auxiliares con toques de *Variable Compleja*, se podrá proveer una prueba que englobará algún caso más que el resultado de partida en el caso particular del grupo $\mathbf{SO}(N)$. Asimismo, se completarán los casos no contemplados por el resultado principal haciendo uso básico de estimaciones de sumas exponenciales.

En el segundo Capítulo se rescatará el famoso Teorema de los Números Primos en Progresiones Aritméticas. Una vez que se constataron pruebas analíticas a través de la *Variable Compleja* para su análogo sin progresiones aritméticas y para él mismo, surgió un interés por buscar alguna prueba elemental, es decir, que solo necesitara el puro manejo de las sumas involucradas sin recurrir a herramientas más sofisiticadas. Una vez se consiguieron, la complejidad y la extensión de tales pruebas las hizo caer en desuso, pasando a ser el objetivo encontrar un equilibrio entre la extensión y el uso de técnicas complejas. En este sentido, Iwaniec dio una prueba relativamente breve y muy simple para el caso sin progresiones aritméticas. Puesto que buscando en la literatura no se ha encontrado ninguna aplicación del método de Iwaniec a las progresiones aritméticas, este Capítulo se ocupará de ello. El punto clave será la búsqueda de cotas adecuadas para las funciones involucradas que conduzcan a un desarrollo asintótico satisfactorio.

En el tercer Capítulo se realizará un homenaje al recientemente fallecido profesor Javier Cilleruelo intentando dar luz a una de las últimas conjeturas que propuso acerca de los conjuntos de sumas de divisores simétricos de un número natural. En un intento por esclarecer la estructura de tales conjuntos y las ecuaciones diofánticas que los rigen, se apelará a objetos tan diversos como ecuaciones de Pell, curvas elípticas o superficies algebraicas, que aunque no cerrarán por completo el problema, ofrecerán una visión muy clara de cómo un simple juego de números puede convertirse en un problema conjetural fuerte, hecho muy frecuente en *Teoría de Números*, donde los enunciados más cortos, entendibles y bellos dan lugar a pruebas de extraordinaria dificultad y que apelan a técnicas insospechadas que aparentemente no tendrían por que ver nada con los mismos.

Los tres Capítulos mencionados conformarán un compendio de resultados auxiliares que sustentarán las pruebas de los resultados principales y otorgarán a este trabajo de un carácter lo más autocontenido posible, dejando los aspectos que se desvían de cada uno de los objetivos, bien por su dificultad o grado de tecnicismo, para el lector que desee profundizar en su lectura.

Abstract

Number Theory is an almost unattainable discipline within Mathematics and deals with an infinity of phenomena and problems that arise when studying the different numerical sets. This thesis presents three particular contexts (distributed in three respective Chapters) where a subtle contact of this discipline with others such as *Complex Analysis*, *Fourier Analysis*, *Numerical Analysis* or *Algebraic Geometry* is present; sample of the interaction between different techniques that allow obtaining results like those that will occur.

In the first Chapter, we will analyze the phenomenon of the distribution of the spectrum of the Laplace-Beltrami Operator (Weyl's Law) when defined over the classical Lie groups considered as Riemannian varieties. In such a context, *Spectral Theory* can be applied. Although the starting point is an existing result concerning that distribution, the location of a gap in certain inequality will lead to reformulate the proof in terms of a tool coming from *Number Theory*: modular forms. Thanks to this tool and other auxiliary results with a bit of *Complex Analysis*, it will be possible to prove some more cases than the starting result does in the particular case of the group $\mathbf{SO}(N)$. Besides, cases not covered by the main result will be completed using basic estimates of exponential sums.

In the second Chapter, we will rescue the famous Theorem of the Prime Numbers in Arithmetic Progressions. Once analytical proofs were found by using *Complex Analysis* for its analogue without arithmetic progressions and for itself, an increasing interest in looking for some elementary proof, that is, pure handling of the involved sums with no other more sophisticated tools, appeared. Once those proofs were obtained, their complexity and extension made them fall into disuse, the next goal being to find a balance between the extension and the use of complex techniques. In this direction, Iwaniec gave a relatively short and very simple proof for the case without arithmetic progressions. Since no reference to any application of the Iwaniec method for arithmetic progressions has been found, this Chapter will deal with the matter. The key point will be to find suitable bounds for the involved functions that will lead to satisfactory description of the asymptotic behaviour.

In the third Chapter, we will pay a tribute to the recently deceased Professor Javier Cilleruelo and try to clarify one of the last conjectures that he stated about the sets of sums of symmetrical divisors of a natural number. In an attempt to figure out their structure and the diophantine equations associated, we appeal to objects as diverse as Pell's equations, elliptic curves or algebraic surfaces, which do not completely close the problem but offer a very clear vision of how a simple game of numbers can become a strong conjectural problem. This kind of facts is very frequent in *Number Theory*, where the shortest, understandable and beautiful statements give rise to extraordinary difficult proofs by referring to unsuspected techniques that apparently would not have to do anything with them in principle.

The three aforementioned Chapters will conform a compendium of auxiliary results that will support the proofs of the main ones and give this thesis a character as self-contained as possible, leaving those aspects far from each of the objectives, either because of their difficulty or degree of technicality, to the reader who wants to deepen into the reading.

Agradecimientos

Durante los cinco años que he podido desarrollar mi formación e investigación en esta fase de Doctorado han sido muchos los acontecimientos que han marcado el rumbo de los mismos. Enumerarlos todos llenarían las mismas páginas de esta tesis. Pero aún más importante que los hechos han sido las personas con la que me he cruzado en este camino las que han posibilitado escribir estas líneas que marcan el final de una de las etapas más emocionantes de mi carrera académica. Es por ello que me gustaría dedicar estas palabras a todas esas personas que de forma directa o indirecta han participado e influido en esta tesis.

En primer lugar, me gustaría agradecer al profesor Javier Cilleruelo la oportunidad y la puerta de entrada que me ofreció al Doctorado y sin cuyo apoyo y formación inicial no habría vivido esta etapa. Espero haber correspondido y hecho honor de alguna forma a su memoria a través del tercer Capítulo de este trabajo. Tras su desafortunado fallecimiento, me gustaría agradecer al profesor Fernando Chamizo por su incontable paciencia con todas mis limitaciones y obstáculos que he podido pasar gracias a su magistral tutela, ayuda y consejo. Sin duda un porcentaje realmente considerable de esta tesis se debe a su esfuerzo por guiarme a través de toda la variedad de campos en los que nos hemos aventurado, sin contar todos aquellos aspectos que aunque no han quedado recogidos en este trabajo final, han formado parte de mi formación y trabajo subyacente.

Aparte de los que han sido mis tutores académicos y por tanto influencia directa en el desarrollo de esta tesis, me gustaría agradecer de forma particular a todas las personas que forman parte de mi familia, sin cuyo extraordinario apoyo moral y económico no habría sido posible continuar en el tiempo todo este proceso. Una mención especial a mis padres, que han sido en unas ocasiones cómplices de los buenos momentos y en otras, víctimas de los malos. De la misma forma me gustaría agradecer a mis hermanas, mis tías y tíos, mis abuelas y abuelos (con un recuerdo especial para los que ya no están) y a todos los miembros de mi familia que me han brindado su apoyo y con los que he compartido mis progresos en esta etapa.

No me olvido del inmenso grupo de amigos y personas especiales que ya conocía y he podido conocer a lo largo de estos cinco años. Ellos han contribuido en muchas formas a hacer de este camino algo más ameno y divertido. Para no extenderme demasiado, un recuerdo a mis compañeros y amigos de carrera y de mi estancia durante seis años en Sevilla. Me llevé en su momento a Madrid muy buenos recuerdos de todos ellos y siempre los tendré presentes. Una mención especial a mis amigas Lucía, Rebeca, Ana Mariam, Isabel y María, por los grandes momentos que hemos compartido, así como a mis compañeros de estudios Elena, Javi, Luismi, Manoli, Almudena, Lidia, Carlos, María Luisa y tantos otros. Ya en mi etapa de Doctorado en Madrid, hago mención a mis compañeros de residencia de la UAM Indira, Miguel, Emma, Elisabeth, María José, María, Roberto, Ángel, Dani, Noelia, Diego, Javi, José, Laura... y a mis compañeros académicos del ICMAT y a todos los que he podido conocer en todas las Jornadas, Congresos y Seminarios en estos cinco años. He podido conocer a grandes matemáticas y matemáticos cuya experiencia me ha encantado conocer y compartir. También quiero agradecer a mi Agrupación Musical por formar parte de mis momentos de desconexión y que gracias a la música y a su amistad he podido sobrellevar los momentos de estrés y seguir evolucionando en esa disciplina que forma parte de mis pasiones. Por último, agradecer por el mismo motivo a mi entrenador en la UAM Diego por todo su grandísimo apoyo y su dedicación, así como a todos mis amigos y profesores de la Escuela de Chino Bunkyo, una gran familia con la que he disfrutado del aprendizaje de un nuevo idioma totalmente desconocido para mí como es el chino mandarín. Un recuerdo especial para su director Kwang Fu, mis profesores Tania, Shu Fen y Cristina, así como para Rita y Jacky, dos amigas especialmente queridas.

Sé que me dejo por el camino a muchas personas más que me han acompañado y aprovecho para hacer constar mi agradecimiento a todos ellos. Como última mención, a Rafa, mi mejor amigo desde hace quince años y con el que he tenido vivencias de todas las formas, tamaños y colores, y a Flavio, una persona muy especial que en estos últimos meses, cuando la presión y el estrés han sido mayores, me ha apoyado y ayudado desde el minuto cero cada

vez que lo he necesitado.

Un saludo para todos vosotros y todo mi cariño, admiración y respeto.

José

Capítulo 0

Rudimentos de Teoría de Números

En el campo de la *Teoría de Números*, y especialmente en su vertiente analítica, existen unos aspectos básicos que suponen la base y el punto de partida para el estudio de todos los fenómenos de los que se ocupa, y constituyen un conjunto de herramientas que deben asimilarse correctamente antes de entrar en cuestiones más avanzadas y específicas (en particular, las de este documento). En este Capítulo introductorio se presentarán todos aquellos resultados que serán dados por conocidos y serán empleados en los argumentos de las pruebas del resto de Capítulos. Como notaciones básicas previas que se tomarán se dirá que $n \mid m$ si n *divide a* m, $n \nmid m$ si n *no divide a* m, $\mathrm{mcd}(n,m)$ será el *máximo común divisor* de n y m, y $n \equiv r \,(\mathrm{mod}\, m)$ si n *es congruente con* r *módulo* m. Asimismo, se denotará por $\lfloor x \rfloor$ y $\{x\}$ a las *partes entera y fraccionaria* de x, respectivamente. Las pruebas de todos los resultados aquí enunciados pueden ser consultados en referencias como [**?**], [**?**] y en muchos textos elementales de *Teoría de Números*.

A. Funciones aritméticas. Sea n un número natural. Las llamadas *funciones aritméticas* conforman el objeto inicial de estudio y fundamentación de la *Teoría Analítica de Números*. Entre otras, serán utilizadas las siguientes:

Función de Möbius : $$\mu(n) := \begin{cases} 1 & \text{si } n = 1, \\ (-1)^r & \text{si } n = p_1 \cdots p_r, \quad p_i \neq p_j, \\ 0 & \text{en otro caso.} \end{cases}$$

Función indicatriz de Euler : $$\varphi(n) := \sum_{\substack{m \leq n \\ \mathrm{mcd}(m,n)=1}} 1.$$

Función de von Mangoldt : $$\Lambda(n) := \begin{cases} \log p & \text{si } n = p^a,\ (a \geq 1) \\ 0 & \text{en otro caso.} \end{cases}$$

Función omega : $$\omega(n) := \sum_{p \mid n} 1.$$

Funciones identidad y constante 1 $$id(n) := \begin{cases} 1 & \text{si } n = 1, \\ 0 & \text{en otro caso.} \end{cases} \qquad \mathbf{1}(n) := 1 \text{ para todo } n.$$

Caracteres de Dirichlet módulo q $\chi(n)$ (véase el Capítulo 2)

Si f es una función aritmética, se dice que f es *multiplicativa* si $f(mn) = f(m)f(n)$ para todo m coprimo con n, y *completamente multiplicativa* si $f(mn) = f(m)f(n)$ para cualesquiera m y n. De entre las funciones anteriores, μ, φ, id y $\mathbf{1}$ son multiplicativas por construcción. Nótese que si f es una función multiplicativa, entonces $f(1) = 1$, ya que $f(n)$ no es idénticamente nula para todo n y $f(n) = f(n \cdot 1) = f(n)f(1)$. Por tanto, si se aplica este criterio, las funciones Λ y ω no son multiplicativas, ya que $\Lambda(1) = 0 = \omega(1)$. Es posible comprobar que las funciones μ, φ y Λ verifican directamente a partir de su definición las identidades:

$$\sum_{d \mid n} \mu(d) = id(n), \qquad \sum_{d \mid n} \varphi(d) = n. \tag{1}$$

B. Convolución. Las funciones aritméticas no son solo interesantes aisladamente. Las interacciones entre ellas ofrecen todo un abanico de resultados cuya influencia alcanza a multitud de problemas estudiados en *Teoría de Números*. La forma más común de interacción es una especie de multiplicación entre distintas funciones aritméticas. Si f y g son dos funciones aritméticas, su *producto de convolución* es otra función denotada por $f * g$ y definida de la siguiente forma:

$$(f * g)(n) = \sum_{d|n} f(d) g\left(\frac{n}{d}\right).$$

La convolución entre funciones aritméticas es conmutativa y asociativa, aunque lo más interesante y útil en la práctica es el hecho de que:

$$f,\, g \text{ multiplicativas} \quad \Rightarrow \quad f * g \text{ multiplicativa.} \tag{2}$$

Como caso particular puede tomarse además $g = \mathbf{1}$, obteniendo que:

$$f \text{ multiplicativa} \quad \Rightarrow \quad \sum_{d|n} f(d) \text{ multiplicativa.} \tag{3}$$

Esto posibilita, una vez establecida una función f definida a través de una convolución $g * \mathbf{1}$, recuperar información sobre g y viceversa a través de la conocida *fórmula de inversión de Möbius*, que sostiene:

$$f(n) = \sum_{d|n} g(d) \quad \Leftrightarrow \quad g(n) = \sum_{d|n} \mu(d) f\left(\frac{n}{d}\right) = \sum_{d|n} f(d) \mu\left(\frac{n}{d}\right). \tag{4}$$

El producto de convolución puede generalizarse a funciones reales o con valores complejos y de ahí al producto de las mismas por funciones aritméticas completamente multiplicativas. La idea general consiste en transformar las condiciones del tipo $d|n$ en otras del tipo $d \leq n$, lo cual es un simple cambio en la forma de contar los divisores d. Como resultado, se pueden obtener fórmulas como:

$$\sum_{n\leq x} \sum_{d|n} f(d) g\left(\frac{n}{d}\right) = \sum_{n\leq x} f(n) \sum_{m\leq \frac{x}{n}} g(m), \qquad \sum_{n\leq x} \sum_{d|n} f(d) = \sum_{n\leq x} f(n) \lfloor \frac{x}{n} \rfloor; \tag{5}$$

Si se consideran f y g funciones reales o con valores en $\mathbb{C}$ definidas en $(0, +\infty)$ con $f(x) = 0 = g(x)$ para todo $0 < x < 1$ y $a(n)$ es completamente multiplicativa, entonces a partir de (5) es posible conseguir un análogo a (4), es decir, una *fórmula de inversión de Möbius generalizada*, la cual se emplea con mayor frecuencia para estudiar sumas parciales de funciones diversas:

$$f(x) = \sum_{n\leq x} a(n) g\left(\frac{x}{n}\right) \quad \Leftrightarrow \quad g(x) = \sum_{n\leq x} \mu(n) a(n) f\left(\frac{x}{n}\right). \tag{6}$$

Otra forma es considerar las parejas de divisores $dd' = n \leq x$ como puntos enteros bajo una hipérbola, lo cual da lugar a otra fórmula para las sumas parciales de la convolución de dos funciones aritméticas $f * g$ que puede ser nombrada como *sumación hiperbólica*:

$$\sum_{n\leq x} (f * g)(n) = \sum_{n\leq a} f(n) G\left(\frac{x}{n}\right) + \sum_{n\leq b} g(n) F\left(\frac{x}{n}\right) - F(a) G(b), \tag{7}$$

donde a y b son dos números reales positivos tales que $ab = x$ y

$$F(x) = \sum_{n\leq x} f(n), \qquad G(x) = \sum_{n\leq x} g(n).$$

C. Series de Dirichlet. Uno de los objetos matemáticos más importantes del cual las funciones aritméticas forman parte y que está detrás de grandes resultados de la *Teoría de Números* es una cierta serie que se le puede asociar a una función aritmética f dada. Dicha serie se denomina *serie de Dirichlet* y constituye una función de la variable compleja $s = \sigma + it$ definida como:

$$\sum_{n=1}^{\infty} \frac{f(n)}{n^s}.$$

Las series de Dirichlet están bien definidas como funciones de s en sus respectivas regiones de convergencia. Como norma general, si la serie

$$\sum_{n=1}^{\infty} \left| \frac{f(n)}{n^s} \right|$$

no converge para todo s ni diverge para todo s, entonces puede probarse que existe un número real σ_a (*abscisa de convergencia absoluta*) tal que la serie de Dirichlet converge absolutamente si $\sigma > \sigma_a$ y no converge absolutamente si $\sigma < \sigma_a$. Por otra parte, gracias a la convergencia absoluta es posible multiplicar dos series de Dirichlet:

$$F(s) = \sum_{n=1}^{\infty} \frac{f(n)}{n^s}, \quad (\sigma > \sigma_a); \qquad G(s) = \sum_{m=1}^{\infty} \frac{g(m)}{m^s}, \quad (\sigma > \sigma_b);$$

y reordenar los términos arbitrariamente sin alterar el valor de la suma, de manera que el producto es la serie de Dirichlet asociada a la convolución de las funciones aritméticas implicadas :

$$F(s)G(s) = \sum_{n=1}^{\infty} \frac{(f * g)(n)}{n^s}. \tag{8}$$

Esta nueva serie estará bien definida en la región de convergencia absoluta común a las dos series de partida. Por otra parte, un asunto más delicado que también atañe al hecho de relacionar dos series de Dirichlet $F(s)$ y $G(s)$ es ver qué ocurre cuando se tiene la igualdad entre ambas bajo circunstancias particulares. Más concretamente, se puede establecer que si $F(s)$ y $G(s)$ poseen la misma abscisa de convergencia absoluta y $F(s) = G(s)$ para todo s en una sucesión $\{s_j\}$ tal que $\sigma_j \longrightarrow +\infty$ cuando $j \to \infty$, entonces las funciones aritméticas involucradas cumplen que $f(n) = g(n)$ para todo n. Esta condición de unicidad aparenta ser un análogo al *Principio de Identidad* que se tenía para las series de potencias , aunque sus pruebas respectivas son diferentes, algo que no es extraño ya que en esencia, las series de potencias y las series de Dirichlet son objetos completamente distintos.

Como caso particular, tomando las funciones aritméticas $f(n) = \mathbf{1}(n)$ y $f(n) = \chi(n)$, se obtienen respectivamente la *función zeta de Riemann* y la *función L de Dirichlet asociada a* χ (véase el Capítulo 2):

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}, \qquad L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}.$$

Ambas series tienen abscisa de convergencia $\sigma_a = 1$. Como por (1) se tiene que $\mathbf{1} * \mu = \mu * \mathbf{1} = id$, aplicando (8) al caso $f(n) = \mathbf{1}(n)$ y $g(n) = \mu(n)$ el producto de las series de Dirichlet asociadas es:

$$\zeta(s) \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} = \sum_{n=1}^{\infty} \frac{id(n)}{n^s} = 1.$$

Esto demuestra en particular que para $\sigma > 1$:

$$\frac{1}{\zeta(s)} = \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s}. \tag{9}$$

Las series de Dirichlet, al ser funciones de la variable compleja s, pueden admitir una función derivada, que viene dada la serie de Dirichlet:

$$\sum_{n=1}^{\infty} \frac{f(n) \log n}{n^s}.$$

Tomando de nuevo $f(n) = \mathbf{1}(n)$ y $f(n) = \mu(n)$, las derivadas de las series asociadas a cada una corresponden respectivamente por definición y por (8) a:

$$\zeta'(s) = \sum_{n=1}^{\infty} \frac{\log n}{n^s}; \qquad \left(\frac{1}{\zeta(s)}\right)' = \sum_{n=1}^{\infty} \frac{\mu(n) \log n}{n^s}. \tag{10}$$

Precisamente la serie de Dirichlet asociada a $(1/\zeta(s))'$ puede emplearse para establecer una convolución con la función $\Lambda(n)$, que no era multiplicativa por lo que a priori no cabía considerar un producto de convolución donde estuviera involucrada. Sin embargo, se pueden probar las identidades válidas para todo n:

$$(\mathbf{1} * \Lambda)(n) = \log(n), \qquad (\mu * \log)(n) = \Lambda(n), \qquad -\mu(n) \log(n) = (\mu * \Lambda)(n). \tag{11}$$

Estos productos de convolución serán especialmente útiles en desarrollos posteriores.

D. Productos de Euler. Si f es una función aritmética multiplicativa, entonces la suma de la serie de Dirichlet asociada a ella puede expresarse como un producto infinito absolutamente convergente definido únicamente sobre todos los primos de forma que para $\sigma > \sigma_a$:

$$\sum_{n=1}^{\infty} \frac{f(n)}{n^s} = \prod_p \left(1 + \frac{f(p)}{p^s} + \frac{f(p^2)}{p^{2s}} + \dots\right).$$

Si además f es completamente multiplicativa, el producto se puede escribir en términos de una serie geométrica, por lo que puede reducirse a la expresión:

$$\sum_{n=1}^{\infty} \frac{f(n)}{n^s} = \prod_p \frac{1}{1 - f(p)p^{-s}}.$$

En ambos casos, el producto resultante se denomina *producto de Euler* asociado a la serie de Dirichlet. Aplicando esto una vez más a las funciones $\mathbf{1}(n)$ y $\chi(n)$, se obtienen los respectivos productos de Euler para $\zeta(s)$ y $L(s,\chi)$, válidos para $\sigma > 1$:

$$\zeta(s) = \prod_p \frac{1}{1 - p^{-s}}; \qquad L(s,\chi) = \prod_p \frac{1}{1 - \chi(p)p^{-s}}. \tag{12}$$

E. Fórmulas de sumación. En la *Teoría de Números* aparecen de forma constante sumas de la forma:

$$\sum_{n \le x} a(n)f(n),$$

donde $a(n)$ es una función aritmética. En la mayoría de casos estas sumas no se calculan de forma explícita, sino que se busca estimarlas de una forma adecuada como una serie de términos principales y un término de error para estudiar un determinado fenómeno o comportamiento. Para poder hacerlo existen varios métodos que producen desarrollos más o menos precisos dependiendo de las funciones involucradas. Como primer método, si $A(x)$ es la suma parcial de $a(n)$ dada por:

$$A(x) := \sum_{n \le x} a(n),$$

donde $A(x) = 0$ si $x < 1$, agrupando de cierta forma los términos de la serie se verifica la fórmula de *sumación parcial*:

$$\sum_{n \le x} a(n)f(n) = A(x)f(\lfloor x \rfloor + 1) + \sum_{n \le x} A(n)(f(n) - f(n+1)). \tag{13}$$

Si además f es una función con derivada continua en el intervalo $[y,x]$ para $0 < y < x$, entonces es posible aprovechar la relación entre sumas e integrales para obtener la fórmula de *sumación de Abel*:

$$\sum_{y < n \le x} a(n)f(n) = A(x)f(x) - A(y)f(y) - \int_y^x A(t)f'(t)\,dt. \tag{14}$$

Por otra parte, tomando $a(n) = 1$ en (13) y haciendo uso de la fórmula de integración por partes, se deduce la fórmula de *sumación de Euler*:

$$\sum_{y < n \le x} f(n) = \int_y^x f(t)\,dt + \int_y^x (t - \lfloor t \rfloor)f'(t)\,dt + f(x)(\lfloor x \rfloor - x) - f(y)(\lfloor y \rfloor - y). \tag{15}$$

Introduciendo la función $\psi(x) := x - \lfloor x \rfloor - 1/2$ y aplicando (15), de nuevo para f una función con derivada continua en el intervalo $[y,x]$ se obtiene la fórmula de *sumación de Euler-McLaurin*:

$$\sum_{y < n \le x} f(n) = \phi(y)f(y) - \phi(x)f(x) + \int_y^x (f(t) + \phi(t)f'(t)\,dt. \tag{16}$$

Por último, dada una función f real es posible establecer cierta relación entre los valores en los enteros de f y de su *transformada de Fourier*:

$$\mathcal{F}[f](\xi) = \hat{f}(\xi) := \int_{-\infty}^{\infty} f(x)e^{-2\pi i \xi x}\,dx.$$

Dicha relación corresponde a la fórmula de *sumación de Poisson*:

$$\sum_{n\in\mathbb{Z}} f(n) = \sum_{m\in\mathbb{Z}} \hat{f}(m). \tag{17}$$

Si f es una función vectorial, esta relación puede extenderse a tuplas de enteros.

F. Notaciones $\mathcal{O}$ y o de Landau. Al aplicar los métodos de sumación anteriores a sumas particulares se obtienen términos principales explícitos, que rigen el comportamiento esencial de la suma, y términos de error propios de todo método aproximado. La forma de expresar estos términos de error de una manera cómoda y manejable es a través de una notación introducida por Landau. Sean f y g dos funciones definidas en un conjunto A. Las relaciones asintóticas entre f y g pueden plasmarse de diferentes formas:

$$\begin{aligned} &f = \mathcal{O}(g) \text{ o } f \ll g && \text{si existe una constante } C \text{ tal que } |f(x)| \le C|g(x)| \text{ para todo } x \in A, \\ &f = o(g) && \text{si } \lim_{x\to x_0} \frac{f(x)}{g(x)} = 0, \\ &f \sim g && \text{si } \lim_{x\to x_0} \frac{f(x)}{g(x)} = 1. \end{aligned} \tag{18}$$

Al trabajar con términos de error expresados a través de la notación $\mathcal{O}$ y o, se pueden realizar las siguientes operaciones:

$$\begin{aligned} &(\textit{Simplificación de constantes}) && \mathcal{O}(Cg) = \mathcal{O}(g) \text{ y } o(Cg) = o(g) \text{ si } C > 0. \\ &(\textit{Transitividad}) && f = \mathcal{O}(g),\, g = \mathcal{O}(h) \Rightarrow f = \mathcal{O}(h), \quad f = o(g),\, g = o(h) \Rightarrow f = o(h); \\ &(\textit{Multiplicación}) && f_j = \mathcal{O}(g_j),\, o(h_j),\, j = 1,2 \Rightarrow f_1 f_2 = \mathcal{O}(g_1 g_2),\, o(h_1 h_2); \\ &(\textit{Extracción de factores}) && f = \mathcal{O}(gh) \Rightarrow f = g\mathcal{O}(h), \quad f = o(gh) \Rightarrow f = go(h); \\ &(\textit{Sumación de términos } \mathcal{O}) && f_j = \mathcal{O}(g_j),\, 1 \le j \le n \text{ y las constantes no dependen de } j \\ &&& \qquad \Rightarrow \sum_{j=1}^{n} f_j(x) = \mathcal{O}\left(\sum_{j=1}^{n} |g_j(x)|\right); \\ &(\textit{Integración de términos } \mathcal{O}) && f = \mathcal{O}(g) \text{ para } x \ge x_0 \text{ y } f,\, g \text{ son integrables} \\ &&& \qquad \Rightarrow \int_{x_0}^{x} f(y)\,dy = \mathcal{O}\left(\int_{x_0}^{x} |g(y)|\,dy\right). \end{aligned} \tag{19}$$

Nótese que el empleo de los términos $\mathcal{O}$ debe hacerse con cuidado. Dado un término de error $\mathcal{O}(f)$, es posible escribir $\mathcal{O}(f) = \mathcal{O}(g)$ si para $x \ge x_0$ se tiene $|f(x)| \le C|g(x)|$ para cierta constante positiva. Sin embargo esta relación no es simétrica, es decir, $\mathcal{O}(g) \ne \mathcal{O}(f)$. Por otra parte, para toda función ϕ, se tiene que $o(\phi) = \mathcal{O}(\phi)$, ya que si $f/\phi \longrightarrow 0$, entonces en particular f/ϕ está acotada a partir de cierto valor en adelante. Pero de nuevo no ocurre lo contrario, es decir, $\mathcal{O}(\phi) \ne o(\phi)$, ya que el hecho de que f/ϕ esté acotada no significa necesariamente que $f/\phi \longrightarrow 0$.

G. Aplicación de las fórmulas de sumación. Gracias a los métodos de sumación descritos en el apartado **E** y al uso de la notación $\mathcal{O}$ y sus propiedades en (19) es posible deducir los siguientes desarrollos asintóticos para $x \ge 1$, que serán utilizados en los demás Capítulos:

$$\sum_{n\le x} \log n = \log\lfloor x\rfloor! = x\log x - x + \mathcal{O}\left(\log x\right), \tag{20}$$

$$\sum_{n\le x} \frac{1}{n} = \log x + \gamma + \mathcal{O}\left(\frac{1}{x}\right), \tag{21}$$

$$\sum_{n\le x} \frac{\phi(n)}{n} = \frac{6x}{\pi^2} + \mathcal{O}(\log x), \tag{22}$$

$$\sum_{n\le x} \frac{1}{n^2} = \zeta(2) + \mathcal{O}\left(\frac{1}{x}\right) = \frac{\pi^2}{6} + \mathcal{O}\left(\frac{1}{x}\right), \tag{23}$$

$$\sum_{n\leq x}\frac{1}{\sqrt{n}}=2\sqrt{x}+A+\mathcal{O}\left(\frac{1}{\sqrt{x}}\right). \tag{24}$$

En la identidad (21), la constante γ es la llamada *constante de Euler*, que verifica:

$$\lim_{n\to\infty}\log n\prod_{p\leq n}\left(1-\frac{1}{p}\right)=e^{-\gamma}. \tag{25}$$

H. Método de pares de exponentes para sumas exponenciales. Sea f una función real. El objetivo es estimar sumas del tipo:

$$S:=\sum_{n\in(a,b]}e^{2\pi i f(n)}.$$

Como $|e^{2\pi i f(n)}|=1$ para todo n, la *desigualdad triangular* permite estimar el valor de S obteniendo la estimación trivial $|S|\leq b-a$. Para obtener cotas que sean mejores que la trivial hay que considerar un balance entre la contribución del número de términos involucrados en S, es decir, del tamaño de $b-a$, y la contribución de la oscilación que pudiera tener f, lo cual puede analizarse a través de sus derivadas. De esta forma surge el llamado *Método de pares de exponentes*, que prueba estimaciones del tipo:

$$S\ll M^k(b-a)^\ell, \tag{26}$$

con $f'\leq M$ en $(a,b]$. Se dice que si la estimación es cierta, entonces el par (k,ℓ) es un *par de exponentes*. Lo más interesante es que dado un par de exponentes conocido es posible obtener nuevos pares utilizando los procesos A y B, basados en la *desigualdad de Weyl-van der Corput* y en la *fórmula de sumación de Poisson*, respectivamente:

$$A(k,\ell)=\left(\frac{k}{2k+2},\frac{k+\ell+1}{2k+2}\right),\qquad B(k,\ell)=\left(\ell-\frac{1}{2},k+\frac{1}{2}\right). \tag{27}$$

Puesto que la estimación trivial de S correspondería al par $(0,1)$, puede tomarse como punto de partida de aplicación de los procesos A y B.

Capítulo 1

La Ley de Weyl sobre el grupo especial ortogonal $\mathbf{SO(N)}$

§1. La Ley de Weyl y el origen del problema

A. Ley de Weyl sobre variedades Riemannianas compactas - Grupos de Lie clásicos. Uno de las muchos aspectos que pueden estudiarse en *Teoría de Operadores* es la distribución del *espectro* (es decir, los autovalores) de un operador determinado aplicado sobre una variedad compacta o con frontera determinada. Dada la enorme casuística de tipos de operadores y variedades a las que se pueden aplicar, el espectro en general puede adquirir comportamientos muy diferentes. Para especificar el contexto en el que se va a trabajar en este Capítulo, se considerará M una variedad Riemanniana compacta de dimensión d, g una métrica Riemanniana definida sobre M y se buscará estudiar que ocurre con el espectro del *operador de Laplace-Beltrami* aplicado sobre M: [1]

$$-\Delta_g = \frac{1}{\det(g)} \sum_{i,j=1}^{d} \frac{\partial}{\partial x_i} \left(\sqrt{\det(g)} g^{ij} \frac{\partial}{\partial x_j} \right).$$

Nótese que este operador es una generalización del concepto de laplaciano, ya que en particular si la métrica Riemanniana g que se escoge es la euclídea, el operador se reduce al laplaciano del cálculo diferencial en $\mathbb{R}^d$. En este contexto particular, las características de $-\Delta_g$ hacen que su espectro posea buenas propiedades. Más concretamente, para cada $\lambda \in \mathbb{C}$ se considera la ecuación $-\Delta_g u = \lambda u$. Al ser $-\Delta_g$ un operador autoadjunto,[2] entonces $\lambda \in \mathbb{R}$ y multiplicando la ecuación por u e integrando sobre M puede verse que $\lambda \geq 0$. Para finalizar, como M es compacta, el espectro es un conjunto discreto y ello implica que los autovalores pueden ser enumerados de forma que $\lambda = \lambda_n$, repitiendo λ tantas veces como indique su multiplicidad.

El hecho de que los autovalores sean reales, no negativos y puedan ser enumerados da lugar a que pueda describirse un comportamiento asintótico para ellos. En 1949 [**?**] se consiguió dar una prueba con este grado de generalidad de un resultado enunciado por Weyl en 1911 sobre dicho comportamiento:

Teorema 1.1 *(Ley de Weyl) Sea M una variedad Riemanniana compacta. Dado $\lambda \in \mathbb{R}$, sea la función contadora de los autovalores del operador $-\Delta_g$ definido sobre M:*

$$\mathcal{N}(\lambda) := \sum_{\lambda_n \leq \lambda} 1.$$

Entonces $\mathcal{N}(\lambda)$ cumple:

$$\lim_{\lambda \to \infty} \lambda^{-\frac{d}{2}} \mathcal{N}(\lambda) = \frac{\mathrm{Vol}_g(M)\omega_d(1)}{(2\pi)^d},$$

[1] Dada una variedad M de dimensión d, una *métrica Riemanniana* sobre M constituye básicamente una forma de medir sobre M. Toda métrica Riemanniana g puede expresarse como:

$$g = \sum_{i,j=1}^{d} g_{ij} \mathrm{d}x_i \otimes \mathrm{d}x_j,$$

donde g_{ij} son los coeficientes de la métrica. Esta expresión puede verse en forma matricial como $g = (g_{ij})_{d \times d}$, por lo que en la definición de $-\Delta_g$ se denota g^{ij} a las entradas de la matriz g^{-1}.

[2] $\langle -\Delta_g u, v \rangle = \langle u, -\Delta_g v \rangle$ para cualesquiera vectores u, v en M y siendo $\langle \cdot, \cdot \rangle$ el producto interno definido sobre M como $\langle f, g \rangle = \int_M \overline{f} g$.

donde $\mathrm{Vol}_g(M)$ *es el volumen de* M *con respecto a la métrica Riemanniana* g *definida sobre* M*:*

$$\mathrm{Vol}_g(M) = \int_M \sqrt{\det(g)}\, \mathrm{d}x_1 \wedge \cdots \wedge \mathrm{d}x_d,$$

y $\omega_d(1) = |\mathbb{B}_1^d|$ *es el volumen de la bola de dimensión* d *y radio* 1 *en el espacio euclídeo* $\mathbb{R}^d$*.*

Una prueba sucinta de este resultado, que utiliza la formulación variacional del problema $-\Delta_g u = \lambda u$, puede consultarse en [**?**]. En el comportamiento asintótico que se describe para $\mathcal{N}(\lambda)$ aparecerá como es obvio un término de error. El estudio de dicho término de error ha revelado una relación bastante fuerte entre el análisis subyacente tras las ecuaciones de los autovalores, la geometría de la variedad M y la física matemática, tal y como puede verse en [**?**], y en estas interacciones la aritmética realiza un papel significativo, tal y como se muestra en [**?**].

Como pequeño paso inicial, puede precisarse un poco más la formulación del comportamiento asintótico que se enuncia en el Teorema 1.1:

Lema 1.2 *Se verifica:*

$$\omega_d(R) := |\mathbb{B}_R^d| = \frac{2\pi^{\frac{d}{2}} R^d}{d\Gamma\left(d/2\right)}.$$

Demostración. Sea S_r^{d-1} la frontera de la bola $\mathbb{B}_r^d$, es decir, la esfera de dimensión $d-1$ y radio r. Teniendo en cuenta que en general su área, denotada por $|S_r^{d-1}|$, es proporcional a r^{d-1}, se verifica:

$$\omega_d(R) = \int_0^R |S_r^{d-1}|\, dr = |S_1^{d-1}| \int_0^R r^{d-1}\, dr = \frac{|S_1^{d-1}| R^d}{d}.$$

Por tanto, aplicando la definición de la *función gamma de Euler* $\Gamma(s)$ y lo anterior se obtiene realizando el cambio $\|\vec{x}\| = r = \sqrt{t}$:

$$\begin{aligned}\pi^{\frac{d}{2}} = \left(\int_{\mathbb{R}} e^{-x^2}\, dx\right)^d = \int_{\mathbb{R}^d} e^{-\|\vec{x}\|^2}\, d\vec{x} &= \int_0^\infty e^{-r^2} |S_r^{d-1}|\, dr \\ &= |S_1^{d-1}| \int_0^\infty e^{-r^2} r^{d-1}\, dr = \frac{d\omega_d(R)}{2R^d} \int_0^\infty e^{-t} t^{\frac{d}{2}-1}\, dt = \frac{d\omega_d(R)}{2R^d} \Gamma\left(\frac{d}{2}\right),\end{aligned}$$

de donde se concluye el enunciado. □

El objetivo de este Capítulo es estudiar la *Ley de Weyl*, y en particular el término de error en el desarrollo asintótico, cuando se aplica a los llamados *grupos de Lie clásicos*, de entre los cuales se pueden citar, para $N \geq 2$:

$$\mathbf{U}(N) = \{A \in \mathcal{M}_{N\times N}(\mathbb{C}) \,|\, A\overline{A}^t = I_N\}, \quad (\textit{Grupo Unitario})$$

$$\mathbf{SU}(N) = \{A \in \mathcal{M}_{N\times N}(\mathbb{C}) \,|\, A\overline{A}^t = I_N,\, |A| = 1\}, \quad (\textit{Grupo Especial Unitario})$$
$$\mathbf{SO}(N) = \{A \in \mathcal{M}_{N\times N}(\mathbb{R}) \,|\, AA^t = I_N,\, |A| = 1\}, \quad (\textit{Grupo Especial Ortogonal})$$
$$\mathbf{Spin}(N) = \text{ recubrimiento universal de } \mathbf{SO}(N), \quad (\textit{Grupo Espinorial})$$

Esencialmente, un *grupo de Lie* es una variedad diferenciable real o compleja que tiene estructura de grupo y respecto de la que las operaciones de grupo (multiplicación e inversión) son funciones diferenciables o analíticas, según corresponda. De los grupos que se han citado anteriormente, puede verse que $\mathbf{U}(N)$, $\mathbf{SU}(N)$ y $\mathbf{SO}(N)$ son grupos de matrices, mientras que $\mathbf{Spin}(N)$ es el *recubridor universal* de $\mathbf{SO}(N)$, ya que su grupo fundamental es $\pi_1(\mathbf{SO}(N)) \cong \mathbb{Z}_2$, pero esto solo se cumple para $N > 2$. En el caso $N = 2$ se tiene $\mathbf{SO}(2) \cong S^1 \cong \{|z| = 1\}$ (el ángulo de rotación) y $\mathbf{Spin}(2) \cong \mathbb{R}$.

El hecho de que se satisfaga la *Ley de Weyl* en los cuatro grupos anteriores se debe a que como variedades son compactas para todo $N \geq 2$. Como variedades Riemannianas, al aplicar el operador $-\Delta_g$, en todas ellas aparece un espectro dotado de fórmulas explícitas (nada triviales de obtener) para cada uno de los autovalores que lo conforman. En este documento, la atención se centrará en el grupo $\mathbf{SO}(N)$, ya que si se comparan sus fórmulas para los autovalores con las del resto de grupos, representa un caso más complejo por la heterogeneidad de las mismas.

B. Formas modulares. A continuación se presenta uno de los objetos clásicos en *Teoría de Números* cuyas propiedades han suscitado problemas y aplicaciones muy diversas:

Definición 1.3 *Sea el grupo:*

$$\mathbf{SL_2}(\mathbb{Z}) = \left\{ \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathcal{M}_{2\times 2}(\mathbb{Z}) \,|\, \alpha\delta - \beta\gamma = 1 \right\},$$

y sea para cada N natural el subgrupo $\Gamma_0(N) = \{\tau \in \mathbf{SL_2}(\mathbb{Z}) \,|\, \gamma \equiv 0 \,(\mathrm{mod}\, N)\}$. Una forma modular de peso $w \in \mathbb{Q}$ para $\Gamma_0(N)$ es una función $f : \mathbb{H} \longrightarrow \mathbb{C}$, donde $\mathbb{H} = \{z \in \mathbb{C} \,|\, \mathrm{Im}(z) > 0\}$ es el semiplano superior del plano complejo, tal que:

(*A*) *f es holomorfa en $\mathbb{H}$.*

(*B*) *Para toda $\tau \in \Gamma_0(N)$ se tiene: $f(\tau(z)) = f\left(\frac{\alpha z+\beta}{\gamma z+\delta}\right) = \varepsilon_\tau (j_\tau(z))^w f(z)$, donde ε_τ es un número complejo de módulo 1 llamado multiplicador y $j_\tau(z) = \gamma z + \delta$.*

(*C*) *f es holomorfa en sus cúspides.*

En general, las *cúspides* de una forma modular para $\mathbf{SL}_2(\mathbb{Z})$ o de sus subgrupos de índice finito son $\mathbb{Q} \cup \{i\infty\}$. Sin embargo, varias de ellas son equivalentes entre sí bajo la acción del grupo. Para el grupo $\mathbf{SL_2}(\mathbb{Z})$ todas las cúspides son equivalentes a $i\infty$ mientras que en $\Gamma_0(N)$ las cúspides no equivalentes son [**?**] aquellos racionales a/b tales que $b|N$ y $\mathrm{mcd}(a,b) = 1, a \,(\mathrm{mod}\, \mathrm{mcd}(b, N/b))$. Que f sea holomorfa en las cúspides se refiere a que el desarrollo en serie de f en un entorno de cada una de las cúspides no equivalentes (y por tanto en todas) corresponda a una función holomorfa. Dicho desarrollo [**?**], [**?**] es de la forma:

$$f(\sigma_{\mathfrak{a}}(z)) = e^{2\pi i \kappa_{\mathfrak{a}} z} \left(j_{\sigma_{\mathfrak{a}}}(z)\right)^w \sum_{n=0}^{\infty} a_n^{\mathfrak{a}} e^{2\pi i n z},$$

donde $0 \leq \kappa_{\mathfrak{a}} < 1$, los coeficientes $a_n^{\mathfrak{a}}$ dependen de la clase de equivalencia de la cúspide $\mathfrak{a}$ bajo la acción de $\Gamma_0(N)$ y la matriz $\sigma_{\mathfrak{a}}$ (llamada *matriz de escala*) es una matriz tal que $\sigma_{\mathfrak{a}}(i\infty) = \mathfrak{a}$:

$$\sigma_{\mathfrak{a}}(z) = \begin{pmatrix} a\sqrt{m_{\mathfrak{a}}} & \frac{y_0}{\sqrt{m_{\mathfrak{a}}}} \\ b\sqrt{m_{\mathfrak{a}}} & \frac{x_0}{\sqrt{m_{\mathfrak{a}}}} \end{pmatrix},$$

donde $ax_0 - by_0 = 1$ (lo cual es posible dados a y b gracias a la *identidad de Bézout*) y $m_{\mathfrak{a}} = N/\mathrm{mcd}(b^2, N)$.

El estudio de las formas modulares es muy extenso, así como las propiedades que verifican. Para comenzar, se pueden comprobar los siguientes aspectos:

Lema 1.4 *Sea f una forma modular definida sobre $\Gamma_0(N)$. Se cumple:*

(*A*) *f admite una serie de Fourier:*

$$f(z) = \sum_{k=0}^{\infty} a_k e^{2\pi i k z}.$$

(*B*) *La función $g(z) = |\mathrm{Im}(z)|^{\frac{w}{2}} |f(z)|$ es invariante bajo la acción de $\Gamma_0(N)$ y si f es cuspidal, es decir, f tiende a cero en las cúspides, entonces g está acotada.*

(*C*) *Si f es cuspidal, los coeficientes de Fourier verifican $a_k = \mathcal{O}(k^{\frac{w}{2}})$.*

Demostración.

(*A*) La matriz asociada a la transformación traslación $z \to z+1$ es un elemento de $\Gamma_0(N)$ y al aplicarla se obtiene $f(z+1) = f(z)$. Esto quiere decir que f es una función periódica de período 1, por lo que puede asociarsele directamente una serie de Fourier convergente en $\mathbb{H}$.

(*B*) Sea $\tau \in \Gamma_0(N)$. Se verifica directamente que $\mathrm{Im}(\tau(z)) = \mathrm{Im}(z)/|\gamma z + \delta|^2$, por lo que se deduce:

$$g(\tau(z)) = |\mathrm{Im}(\tau(z))|^{\frac{w}{2}} |f(\tau(z))| = \left|\frac{\mathrm{Im}(z)}{|\gamma z+\delta|^2}\right|^{\frac{w}{2}} |\gamma z+\delta|^w |f(z)| = |\mathrm{Im}(z)|^{\frac{w}{2}} |f(z)| = g(z).$$

Por otra parte, si f es cuspidal, para $i\infty$ y el resto de cúspides no equivalentes a/b, cuando $h \to 0^+$ se tiene respectivamente $|f(a/q + ih)| \longrightarrow 0$ y $|f(i/h)| \longrightarrow 0$ exponencialmente. Por otra parte, todo punto de $\mathbb{H}$ se

corresponde mediante los elementos de $\Gamma_0(N)$ con un punto de una cierta región cerrada y conexa llamada *dominio fundamental*. De esta forma, eliminando los entornos abiertos de las cúspides, donde ya se sabe que f tiende a cero, se obtiene una región compacta, donde directamente f es acotada. Por tanto, dado que g es una función continua por definición, esto implica que $g(z) \longrightarrow 0$ en las cúspides de f y g está acotada al eliminar los entornos de las mismas. Así, g es acotada en todo $\mathbb{H}$.

(C) Si f es cuspidal, g es acotada por (B), luego existe una constante C tal que para todo $z \in \mathbb{H}$ se tiene $|f(z)| \leq C\mathrm{Im}(z)^{-\frac{w}{2}}$. Si se toma ahora $z = x + iy$ con y fijo y $0 \leq x < 1$, entonces por la periodicidad de la serie de Fourier, se tiene:

$$|a_k| \leq \frac{1}{2\pi} \int_0^1 |f(x+iy)| e^{2\pi k y}\, dx \leq \frac{C}{2\pi} y^{-\frac{w}{2}} e^{2\pi k y}.$$

Esta desigualdad es válida para todo $y > 0$, y en particular para $y = k^{-1}$ se concluye $a_k = \mathcal{O}(k^{\frac{w}{2}})$. □

A partir de este resultado es posible obtener cotas adecuadas para las sumas parciales de los coeficientes de Fourier de una forma cuspidal [**?**]:

Proposicion 1.5 *Si f es una forma cuspidal, se verifica:*

$$\sum_{k \leq K} a_k = \mathcal{O}\left(K^{\frac{w}{2}} \log K\right).$$

Demostración. Se considera el llamado *núcleo de Dirichlet*:

$$D_K(z) := \sum_{|k| \leq K} e^{2\pi i k z} = \frac{\mathrm{sen}((2K+1)\pi z)}{\mathrm{sen}(\pi z)}.$$

Sea $z = u + i/K$. Entonces:

$$\int_0^1 \left(\sum_{j=1}^{\infty} a_j e^{2\pi i j (u+i/K)} \right) e^{-2\pi i k (u+i/K)}\, du = \begin{cases} a_k & \text{si } k \in \mathbb{N}, \\ 0 & \text{si } k \notin \mathbb{N}. \end{cases}$$

Para $z = u + i/K$ se tiene $g(u + i/K) = |\mathrm{Im}(u + i/K)|^{w/2} |f(u + i/K)| = K^{-w/2} |f(u + i/K)|$. Utilizando esta función, aplicando la identidad anterior con $D_K(z)$ y tomando módulo:

$$\begin{aligned} \left| \sum_{k \leq K} a_k \right| &= \left| \int_0^1 \sum_{j=1}^{\infty} a_j e^{2\pi i j (u+i/K)} \sum_{|k| \leq K} e^{-2\pi i k (u+i/K)}\, du \right| \\ &\leq \int_0^1 \left| f\left(u + \frac{i}{K}\right) \right| \left| D_K\left(-u - \frac{i}{K}\right) \right| du \leq K^{\frac{w}{2}} \int_0^1 g\left(u + \frac{i}{K}\right) \left| D_K\left(-u - \frac{i}{K}\right) \right| du. \end{aligned}$$

La función g está acotada por el Lema 1.4.(B) al ser f una forma cuspidal. Por tanto, para probar el enunciado basta ver que

$$\int_0^1 \left| D_K\left(-u - \frac{i}{K}\right) \right| du \ll \log K.$$

Puesto que D_K es por definición una función par y periódica de período 1, se tienen las siguientes identidades:

$$\begin{aligned} \int_0^1 \left| D_K\left(-u - \frac{i}{K}\right) \right| du &= \int_{-\frac{1}{2}}^{\frac{1}{2}} \left| D_K\left(-u - \frac{i}{K}\right) \right| du = \int_{-\frac{1}{2}}^{\frac{1}{2}} \left| D_K\left(u + \frac{i}{K}\right) \right| du \\ &= \int_{|u| \leq \frac{1}{K}} \left| D_K\left(u + \frac{i}{K}\right) \right| du + \int_{\frac{1}{2} > |u| > \frac{1}{K}} \left| D_K\left(u + \frac{i}{K}\right) \right| du. \end{aligned}$$

Se procede a estimar cada una de las integrales separadamente. Para la primera de ellas se utiliza la propia definición de $D_K(z)$:

$$\int_{|u| \leq \frac{1}{K}} \left| D_K\left(u + \frac{i}{K}\right) \right| du \leq \int_{|u| \leq \frac{1}{K}} \sum_{|k| \leq K} e^{-2\pi \frac{k}{K}}\, du \ll 1 + \frac{1}{K}.$$

Por otra parte, para la segunda integral se recurre a la expresión trigonométrica de $D_K(z)$ y a la identidad:

$$|\operatorname{sen} z| = |\operatorname{sen}(\operatorname{Re}(z))\cosh(\operatorname{Im}(z)) + i\cos(\operatorname{Re}(z))\operatorname{senh}(\operatorname{Im}(z))| = \sqrt{\operatorname{sen}^2(\operatorname{Re}(z)) + \operatorname{senh}^2(\operatorname{Im}(z))}$$

para acotar el numerador y el denominador, obteniendo para $z = u + i/K$ y $K^{-1} < |u| < 1/2$:

$$\left|\operatorname{sen}\left((2K+1)\pi\left(u+\frac{i}{K}\right)\right)\right| \leq \sqrt{1+\operatorname{senh}^2\left(2\pi+\frac{\pi}{K}\right)} \ll 1, \qquad \left|\operatorname{sen}\left(\pi\left(u+\frac{i}{K}\right)\right)\right| \geq |\operatorname{sen}(\pi u)| \gg |u|.$$

Al sustituir estas estimaciones en la segunda integral, se puede deducir:

$$\int_0^1 \left|D_K\left(-u-\frac{i}{K}\right)\right| du \ll 1 + \frac{1}{K} + \int_{\frac{1}{2}>|u|>\frac{1}{K}} \frac{1}{|u|}\, du \ll \log K.$$

y de ahí se concluye el enunciado. □

Para finalizar, se establece una cota superior y una inferior para el cuadrado de los coeficientes de Fourier [**?**]:

Proposicion 1.6 *Si f es una forma cuspidal definida sobre $\Gamma_0(N)$, existe una constante $C > 0$ dependiente de f tal que para K suficientemente grande:*

$$C^{-1} < K^{-w} \sum_{k \leq K} |a_k|^2 < C.$$

Demostración. Dado $a/b \in \mathbb{Q} \cap [0,1]$ [3] un racional irreducible se consideran los intervalos:

$$I_{a/b} = \left\{ x \,:\, \left|x - \frac{a}{b}\right| \leq \frac{1}{b\sqrt{K}},\, C_1\sqrt{K} < b < C_2\sqrt{K} \right\}.$$

Los intervalos $I_{a/b}$ son disjuntos entre sí cuando C_2 es suficientemente pequeño, ya que si $I_{a/b} \cap I_{a'/b'} \neq \emptyset$, se tendría:

$$\frac{1}{bb'} \leq \left|\frac{a}{b} - \frac{a'}{b'}\right| \leq \frac{1}{b\sqrt{K}} + \frac{1}{b'\sqrt{K}},$$

lo que supondría que $1 \leq (b+b')/\sqrt{K} < 2C_2$, es decir, $C_2 > 1/2$. Esto llevaría a contradicción si se tomara C_2 suficientemente pequeño. Tomando dicho C_2, se puede deducir empleando (22) que existe una constante positiva C' tal que:

$$\begin{aligned}\left|\bigcup I_{a/b}\right| &= \left|\bigcup_{\substack{C_1\sqrt{K}<b<C_2\sqrt{K} \\ a/b\in\mathbb{Q}\cap[0,1]\text{ irred}}} \left[-\frac{1}{b\sqrt{K}}, \frac{1}{b\sqrt{K}}\right]\right| = \sum_{\substack{C_1\sqrt{K}<b<C_2\sqrt{K} \\ a/b\in\mathbb{Q}\cap[0,1]\text{ irred}}} \left|\left[-\frac{1}{b\sqrt{K}}, \frac{1}{b\sqrt{K}}\right]\right| = \frac{2}{\sqrt{K}} \sum_{C_1\sqrt{K}<b<C_2\sqrt{K}} \frac{\varphi(b)}{b} \\ &= \frac{2}{\sqrt{K}}\left(\frac{6}{\pi^2}\cdot(C_2-C_1)\sqrt{K} + \mathcal{O}(\log K)\right) > \frac{12(C_2-C_1)}{\pi^2} + C' =: \mu > 0.\end{aligned}$$

Con esto se ha concluido que la medida $|\bigcup I_{a/b}|$ está acotada por una constante $\mu > 0$ que no depende de K. A continuación se procede a demostrar que existe una constante $C_0 > 0$ tal que:

$$\mu_0 := \left|\left\{ x \in \bigcup I_{a/b} \,:\, g\left(x + \frac{i}{K}\right) > C_0 \right\}\right| > 0,$$

con $g(z) = |\operatorname{Im}(z)|^{w/2}|f(z)|$. Tomando $z = u + i/K$ con $u \in \bigcup I_{a/b}$ y usando el desarrollo de f en la cúspide $\mathfrak{a} = a/b$, la función g verifica:

$$\begin{aligned} g\left(u+\frac{i}{K}\right) &= \left|\operatorname{Im}\left(u+\frac{i}{K}\right)\right|^{\frac{w}{2}} \left|f\left(\sigma_{\mathfrak{a}}\left(\sigma_{\mathfrak{a}}^{-1}\left(u+\frac{i}{K}\right)\right)\right)\right| \\ &= \left[m_{\mathfrak{a}}\left(K(bu-a)^2 + \frac{b^2}{K}\right)\right]^{-\frac{w}{2}} \left|\sum_{n=0}^{\infty} a_n^{\mathfrak{a}} e^{2\pi i n \sigma_{\mathfrak{a}}^{-1}(u+i/K)}\right|. \end{aligned}$$

[3] Puesto que f es periódica de período 1, basta estudiar qué ocurre en el intervalo $[0,1]$.

Con estos dos factores obtenidos en $g(u+i/K)$ y con el fin de poder acotar inferiormente la medida μ_0, se procede a dar una cota inferior separadamente para cada uno de dichos factores. Para ello se toman $C_1 = \varepsilon/\sqrt{m_{\mathfrak{a}}}$ y $C_2 = 5\varepsilon/(4\sqrt{m_{\mathfrak{a}}})$ con $\varepsilon > 0$ suficientemente pequeño y los intervalos $I_{a/b} \cdot \varepsilon/(2\sqrt{m_{\mathfrak{a}}})$. Gracias a estas modificaciones se tiene:

$$\left|u - \frac{a}{b}\right| \leq \frac{\varepsilon}{2\sqrt{m_{\mathfrak{a}}}} \cdot \frac{1}{b\sqrt{K}} \quad \left(\text{es decir, } 0 \leq K m_{\mathfrak{a}}(bu-a)^2 \leq \frac{\varepsilon^2}{4}\right),$$

$$\frac{\varepsilon}{\sqrt{m_{\mathfrak{a}}}}\sqrt{K} < b < \frac{5\varepsilon}{4\sqrt{m_{\mathfrak{a}}}}\sqrt{K} \quad \left(\text{es decir, } \varepsilon^2 < \frac{m_{\mathfrak{a}} b^2}{K} < \frac{25}{16}\varepsilon^2\right).$$

Utilizando esto es posible acotar el primero de los factores de $g(u+i/K)$ obteniendo:

$$\left[m_{\mathfrak{a}}\left(K(bu-a)^2 + \frac{b^2}{K}\right)\right]^{-\frac{w}{2}} > \left(\frac{29}{16}\varepsilon^2\right)^{-\frac{w}{2}}.$$

Para hacer algo similar con el segundo factor, se emplea la desigualdad válida para todo l:

$$\left|\sum_{n=1}^{\infty} c_n x^n\right| \geq \left|\sum_{n=1}^{l} c_n x^n\right| - \left|\sum_{n=l+1}^{\infty} c_n x^n\right|.$$

Tomando $l := n_0 = \text{mín}\{n : a_n^{\mathfrak{a}} \neq 0\}$, gracias a la acotación del primer factor se puede deducir:

$$\begin{aligned}\left|\sum_{n=0}^{\infty} a_n^{\mathfrak{a}} e^{2\pi i n \sigma_{\mathfrak{a}}^{-1}(u+i/K)}\right| &= |a_{n_0}^{\mathfrak{a}}| \left|e^{2\pi i n_0 \sigma_{\mathfrak{a}}^{-1}(u+i/K)} + \sum_{n=1}^{\infty} \frac{a_{n+n_0}^{\mathfrak{a}}}{a_{n_0}^{\mathfrak{a}}} e^{2\pi i n \sigma_{\mathfrak{a}}^{-1}(u+i/K)}\right| \\ &\geq |a_{n_0}^{\mathfrak{a}}| \left(e^{-2\pi n_0 [m_{\mathfrak{a}}(K(bu-a)^2 + b^2/K)]^{-1}} - \sum_{n=1}^{\infty} \left|\frac{a_{n+n_0}^{\mathfrak{a}}}{a_{n_0}^{\mathfrak{a}}}\right| e^{-2\pi n [m_{\mathfrak{a}}(K(bu-a)^2 + b^2/K)]^{-1}}\right) \\ &> |a_{n_0}^{\mathfrak{a}}| \left(e^{-2\pi n_0 \varepsilon^{-2}} - \sum_{n=1}^{\infty} \left|\frac{a_{n+n_0}^{\mathfrak{a}}}{a_{n_0}^{\mathfrak{a}}}\right| e^{-2\pi n \frac{16}{29}\varepsilon^{-2}}\right).\end{aligned}$$

Esta cota es positiva, ya que basta tener en cuenta que para $\varepsilon > 0$ suficientemente pequeño, la suma que queda será en módulo menor que $1/2$ por ejemplo. En este sentido, si no se hubiera ajustado la longitud de los intervalos $I_{a/b}$, la cota del primer factor no habría sido suficiente para ver que la cota del segundo factor fuese positiva. Con ambos factores estudiados se concluye que para todo $u \in \bigcup(I_{a/b} \cdot \varepsilon/(2\sqrt{m_{\mathfrak{a}}}))$:

$$g\left(u + \frac{i}{K}\right) > \left(\frac{29}{16}\varepsilon^2\right)^{-\frac{w}{2}} \left(|a_{n_0}^{\mathfrak{a}}| e^{-2\pi n_0 \varepsilon^{-2}} - \sum_{n=n_0+1}^{\infty} |a_n^{\mathfrak{a}}| e^{-2\pi n \frac{16}{29}\varepsilon^{-2}}\right) > 0.$$

Llamando C_0 a esta constante obtenida, se verifica:

$$\mu_0 \geq \left|\bigcup I_{a/b} \cdot \frac{\varepsilon}{2\sqrt{m_{\mathfrak{a}}}}\right| = \frac{\varepsilon}{2\sqrt{m_{\mathfrak{a}}}} \cdot \left|\bigcup I_{a/b}\right| > \frac{\mu\varepsilon}{2\sqrt{m_{\mathfrak{a}}}} > 0.$$

Una vez que se ha probado que $\mu_0 > 0$, puede aprovecharse de la siguiente forma: puesto que g está acotada (Lema 1.4.(B)), g es de cuadrado integrable y por la teoría de *Análisis de Fourier* puede aplicarse la llamada *Identidad de Parseval*, que sostiene que si f es de cuadrado integrable entonces:

$$\int_0^1 |f(t)|^2\, dt = \sum_{k=1}^{\infty} |a_k|^2.$$

Así se llega a:

$$K^w \int_0^1 \left|g\left(u + \frac{i}{K}\right)\right|^2 du = \int_0^1 \left|f\left(u + \frac{i}{K}\right)\right|^2 du = \sum_{k=1}^{\infty} |a_k|^2 e^{-4\pi k/K}.$$

Gracias a que g es acotada y a que $\mu_0 > 0$, existe una constante C' tal que $g > C'$ y:

$$(C')^2 > \int_0^1 \left|g\left(u + \frac{i}{K}\right)\right|^2 du \geq \int_{\bigcup I_{a/b}} \left|g\left(u + \frac{i}{K}\right)\right|^2 du > C_0^2 \mu_0 > 0.$$

Denotando por K_1 y K_2 a las constantes de los extremos, se obtiene:

$$K_1 K^w < \sum_{k=1}^{\infty} |a_k|^2 e^{-4\pi k/K} < K_2 K^w.$$

Utilizando la cota superior con K_2:

$$K_2 K^w > \sum_{k=1}^{\infty} |a_k|^2 e^{-4\pi k/K} \geq e^{-4\pi} \sum_{k \leq K} |a_k|^2.$$

Gracias a esta acotación y tomando $C_2' := e^{4\pi} K_2$, para $M > 0$:

$$\sum_{k>KM} |a_k|^2 e^{-4\pi k/K} \leq \sum_{n=1}^{\infty} \left(\sum_{nKM<k\leq(n+1)KM} |a_k|^2 \right) e^{-4\pi nM} \leq C_2'(KM)^w \sum_{n=1}^{\infty} (n+1)^w e^{-4\pi nM}$$
$$= C_2'(KM)^w e^{-4\pi M} \sum_{n=1}^{\infty} (n+1)^w e^{-4\pi(n-1)M} \leq C_2' S (KM)^w e^{-4\pi M}.$$

Así, utilizando la cota inferior con K_1 y $M > 0$:

$$C_1' K^w := K_1 K^w - C_2' S M^w e^{-4\pi M} K^w < K_1 K^w - \sum_{k>KM} |a_k|^2 e^{-4\pi k/K}$$
$$< \sum_{k=1}^{\infty} |a_k|^2 e^{-4\pi k/K} - \sum_{k>KM} |a_k|^2 e^{4\pi k/K} = \sum_{k\leq KM} |a_k|^2 e^{-4\pi k/K} \leq \sum_{k\leq KM} |a_k|^2.$$

Así, si M es suficientemente grande, $SM^w e^{-4\pi M}$ será suficientemente pequeño para que C_1' sea una constante positiva. De esta forma, observando los extremos de la cadena de desigualdades y renombrando KM por K y C_1'/M^w por C_1', se concluye que para C_1' y C_2' constantes positivas y dependientes de f se tiene:

$$C_1' < K^{-w} \sum_{k\leq K} |a_k|^2 < C_2'.$$

Tomando $C > C_2'$ suficientemente grande tal que $C^{-1} < C_1'$ se tiene el enunciado. □

C. Conexión entre $\mathcal{N}(\lambda)$ y las formas modulares. La relación entre las formas modulares y la función $\mathcal{N}(\lambda)$ puede ser establecida a través de la siguiente función:

Definición 1.7 *Sea A una matriz $n \times n$ de entradas enteras y definida positiva actuando sobre un vector $\vec{m}$ como $A[\vec{m}] = \vec{m}^t A \vec{m}$. Si P es un polinomio en n variables, se define la función theta asociada a P como:*

$$\Theta_P(z) := \sum_{\vec{m}\in\mathbb{Z}} P(\vec{m}) e^{2\pi i \cdot \frac{1}{2} A[\vec{m}] z},$$

donde A es una matriz respecto de la cual P es esférico, es decir:

$$A\left[\frac{\partial}{\partial \vec{x}}\right] P = 0, \qquad \frac{\partial}{\partial \vec{x}} = \left(\frac{\partial}{\partial x_1}, \cdots, \frac{\partial}{\partial x_n}\right)^t.$$

La función theta asociada a P, bajo ciertas condiciones, reúne los requisitos adecuados para ser una forma modular [**?**]:

Teorema 1.8 *Sea A una matriz $n \times n$ de entradas enteras y definida positiva. Sea N_0 un entero positivo tal que $N_0 A^{-1}$ es también una matriz entera. Si tanto A como $N_0 A^{-1}$ poseen entradas diagonales pares y P es esférico respecto de A de grado par ν, entonces la función theta $\Theta_P(z)$ asociada es una forma modular para $\Gamma_0(2N_0)$ de peso $\nu + n/2$, cuspidal si $\nu > 0$.*

La idea de la prueba de este resultado es una aplicación de (17), pudiendo demostrar esencialmente que $\Theta_P(\tau(z)) = \theta(\tau)(\gamma z + \delta)^{\nu+n/2} \Theta_P(z)$ para toda $\tau \in \Gamma_0(2N_0)$, siendo $\theta(\tau)$ un multiplicador que no afecta a las

acotaciones de la Proposición 1.5 y la Proposición 1.6.

Realizando el cambio de variable $Q(\vec{m}) = \frac{1}{2}A[\vec{m}] = k$ se obtiene:

$$\Theta_P(z) = \sum_{k=1}^{\infty} \sum_{Q(\vec{m})=k} P(\vec{m}) e^{2\pi i k z}.$$

La idea que se sigue es tomar como P un polinomio en n variables de grado $\nu > 0$ *homogéneo* (es decir, tal que todos sus monomios son de grado ν), que será esférico con respecto a cierta matriz A. En tal caso, su función theta asociada verificará:

$$\Theta_P(z) = \sum_{k=1}^{\infty} k^{\frac{\nu}{2}} \sum_{Q(\vec{m})=k} P\left(\frac{\vec{m}}{\sqrt{k}}\right) e^{2\pi i k z} = \sum_{k=1}^{\infty} k^{\frac{\nu}{2}} r_n^Q(k, P) e^{2\pi i k z},$$

donde:

$$r_n^Q(k, P) := \sum_{Q(\vec{m})=k} P\left(\frac{\vec{m}}{\sqrt{k}}\right).$$

Bajo las condiciones del Teorema 1.8, Θ_P será una forma cuspidal y así podrá evaluarse el término de error de $\mathcal{N}(\lambda)$, ya que los coeficientes $r_n^Q(k, P)$ estarán de alguna forma involucrados en los cálculos.

Al estudiar la *Ley de Weyl* sobre el grupo $\mathbf{SO}(N)$, los polinomios homogéneos que se manipularán podrán descomponerse en otros con una propiedad adicional que será de utilidad [**?**]:

Proposicion 1.9 *Para $\vec{x} \in \mathbb{R}^n$, sea la norma de $\vec{x}$ definida por $\|\vec{x}\| := \sqrt{x_1^2 + \ldots + x_n^2}$. Todo polinomio homogéneo P de grado g puede escribirse de forma única como:*

$$P(\vec{x}) = \sum_{l=1}^{\lfloor g/2 \rfloor} \|\vec{x}\|^{2l} P_{g-2l}(\vec{x}),$$

donde cada P_j es un polinomio homogéneo y armónico ($\Delta P_j = 0$) de grado j.

Demostración. Sea $\mathcal{P}_n^g$ el espacio de polinomios en n variables reales homogéneos de grado $g \geq 0$ y $\mathcal{H}_n^g$ el subespacio de polinomios en n variables reales homogéneos y armónicos de grado g:

$$\mathcal{H}_n^g := \{P \in \mathcal{P}_n^g \,:\, \Delta P = 0\}.$$

Si $H \in \mathcal{H}_n^g$, entonces $H(\vec{x}) = \|\vec{x}\|^g H(\vec{x}')$, donde $\vec{x} = \|\vec{x}\|\vec{x}'$ y $\vec{x}' \in S^{n-1}$. Por tanto, se considerará a partir de ahora sin pérdida de generalidad que $\mathcal{H}_n^g := \mathcal{H}_n^g|_{S^{n-1}}$. Tomando el producto:

$$\langle f_1, f_2 \rangle_{S^{n-1}} := \frac{1}{\varpi_n} \int_{S^{n-1}} f_1 f_2 \, dS,$$

donde $\varpi_n := |S^{n-1}| = 2\pi^{n/2}/\Gamma(n/2)$, es posible comprobar que si $H_1 \in \mathcal{H}_n^{g_1}$ y $H_2 \in \mathcal{H}_n^{g_2}$ con $g_1 \neq g_2$, se cumple que $\langle H_1, H_2 \rangle_{S^{n-1}} = 0$. La *Identidad de Green* sostiene que si f_1 y f_2 son funciones C^2 en una región Ω, se tiene:

$$\int_\Omega (f_1 \Delta f_2 - f_2 \Delta f_1) \, dV = \int_{\partial\Omega} \left(f_1 \frac{\partial f_2}{\partial \vec{n}} - f_2 \frac{\partial f_1}{\partial \vec{n}} \right) dS,$$

donde dV y dS son los elementos de volumen y superficie y $\partial/\partial\vec{n}$ es la derivada normal en Ω. Para $\Omega = \mathbb{B}^n$ la derivada parcial $\partial/\partial r$ coincide con la derivada normal. Por otra parte, como H_i puede expresarse como $H_i(\vec{x}) = r^{g_i} H_i(\vec{x}')$ para $\vec{x}' \in S^{n-1}$, al aplicar derivada radial y evaluar en $\vec{x}'$ se tendría que $\partial H_i(\vec{x}')/\partial r = g_i H_i(\vec{x}')$. Además $\Delta H_i = 0$ porque H_i es armónico y entonces por la *Identidad de Green*:

$$(g_1 - g_2) \int_{S^{n-1}} H_1 H_2 \, dS = \int_{S^{n-1}} \left(H_1 \frac{\partial H_2}{\partial r} - H_2 \frac{\partial H_1}{\partial r} \right) dS = \int_{\mathbb{B}^n} (H_1 \Delta H_2 - H_2 \Delta H_1) \, d\vec{x} = 0.$$

Con esto se prueba que $\mathcal{H}_n^{g_1} \perp \mathcal{H}_n^{g_2}$ si $g_1 \neq g_2$. En consecuencia, puede verse por inducción que se tiene la siguiente descomposición:

$$\mathcal{P}_n^g = \bigoplus_{0 \leq l \leq \lfloor g/2 \rfloor} \|\vec{x}\|^{2l} \mathcal{H}_n^{g-2l}.$$

En efecto, $\mathcal{P}_n^0 = \mathcal{H}_n^0$ y $\mathcal{P}_n^1 = \mathcal{H}_n^1$, ya que $\Delta P = 0$ para todo polinomio P de grado 0 o 1. Además, si $P \in \mathcal{P}_n^g$ con $g \geq 2$ entonces $\Delta P \in \mathcal{P}_n^{g-2}$. Así, $\Delta \mathcal{P}_n^g \subseteq \mathcal{P}_n^g$ y aplicando dimensiones [4] se cumple que $\dim \mathcal{H}_n^g \geq \dim \mathcal{P}_n^g - \dim \mathcal{P}_n^{g-2}$. Suponiendo que la descomposición que se busca se cumpliera hasta el grado $g-1$, se considera ahora el espacio $\|\vec{x}\|^2 \mathcal{P}_n^{g-2}$, que constituye un subespacio de $\mathcal{P}_n^g$. Utilizando la hipótesis de inducción se verifica:

$$\|\vec{x}\|^2 \mathcal{P}_n^{g-2} = \bigoplus_{0 \leq l \leq \lfloor g/2 \rfloor - 1} \|\vec{x}\|^{2l+2} \mathcal{H}_n^{g-2-2l}.$$

Gracias a esta descomposición y a las relaciones de ortogonalidad entre los diferentes espacios $\mathcal{H}_n^g$, se deduce que $\|\vec{x}\|^2 \mathcal{P}_n^{g-2} \subseteq (\mathcal{H}_n^g)^\perp$, es decir, $\|\vec{x}\|^2 \mathcal{P}_n^{g-2} \perp \mathcal{H}_n^g$ y tomando dimensiones [5] se cumple que $\dim \mathcal{H}_n^g + \dim \mathcal{P}_n^{g-2} \leq \dim \mathcal{P}_n^g$. Uniendo ambas desigualdades obtenidas, se tiene la igualdad y se concluye que $\mathcal{P}_n^g = \mathcal{H}_n^g \oplus \|\vec{x}\|^2 \mathcal{P}_n^{g-2}$. $\square$

El estudio de la Ley de Weyl sobre los grupos de Lie clásicos como $\mathbf{SO}(N)$, $\mathbf{U}(N)$, $\mathbf{SU}(N)$ y $\mathbf{Spin}(N)$ no es nuevo. En [**?**], los autores Morris y Taheri dan una prueba del siguiente resultado:

Teorema 1.10 *Sea $\mathbb{G} = \mathbf{SO}(N)$, $\mathbf{U}(N)$, $\mathbf{SU}(N)$, $\mathbf{Spin}(N)$. Si $d = \dim(\mathbb{G})$ y $n \geq 5$ es el rango de $\mathbb{G}$ (el número máximo de generadores independientes de $\mathbb{G}$), se tiene:*

$$\mathcal{N}(\lambda) = \frac{\mathrm{Vol}(\mathbb{G})}{(4\pi)^{\frac{d}{2}} \Gamma\left(\frac{d}{2}+1\right)} \lambda^{\frac{d}{2}} + \mathcal{O}\left(\lambda^{\frac{d}{2}-1}\right).$$

En la prueba que presentan aprovechan las características intrínsecas de los grupos en cuestión así como el fenómeno de la equidistribución de los puntos de coordenadas enteras en esferas. Más concretamente, si P es un polinomio homogéneo en n variables, la equidistribución de los puntos de coordenadas enteras sobre una esfera n-dimensional puede cuantificarse a través de la expresión:

$$E_n(k,P) := \frac{r_n^{\mathbb{Z}}(k,P)}{r_n^{\mathbb{Z}}(k)} - \frac{1}{\mathrm{Vol}(\mathbb{S}^{n-1})} \int_{\mathbb{S}^{n-1}} P\omega,$$

donde ω es la correspondiente forma de volumen y considerando $Q \equiv \|\cdot\|^2$ aplicada sobre $\vec{x} \in \mathbb{Z}^n$:

$$r_n^{\mathbb{Z}}(k,P) := r_n^Q(k,P), \qquad r_n^{\mathbb{Z}}(k) := r_n^{\mathbb{Z}}(k,1).$$

Los autores toman como referencia una desigualdad referenciada en [**?**], que enuncia la asintótica $E_n(k,P) = \mathcal{O}(k^{-(n-1)/4})$. Si además P es armónico y no constante, la expresión de $E_n(k,P)$ es más simple, ya que:

$$0 = P(0) = \frac{1}{\mathrm{Vol}(S^{n-1})} \int_{S^{n-1}} P\omega.$$

Más aún, en [**?**] se prueba que $r_n^{\mathbb{Z}}(k) \asymp_n k^{\frac{n}{2}-1}$, es decir, existen constantes C_n y C_n' tales que $C_n' k^{n/2-1} < r_n^{\mathbb{Z}}(k) < C_n k^{n/2-1}$. Reuniendo todos estos aspectos, gracias a la Proposición 1.9 que establece la relación entre polinomios homogéneos y armónicos, se puede despejar $r_n^{\mathbb{Z}}(k,P)$ obteniendo para todo P homogéneo y armónico:

$$r_n^{\mathbb{Z}}(k,P) = \mathcal{O}\left(k^{-\frac{n-1}{4}+\frac{n}{2}-1}\right) = \mathcal{O}\left(k^{\frac{n-3}{4}}\right).$$

Esto implica que:

$$\sum_{k \leq K} \left(k^{\frac{\nu}{2}} r_n(k,P)\right)^2 \ll \sum_{k \leq K} k^{\nu+\frac{n-3}{2}} \leq K^{\nu+\frac{n-3}{2}+1} = K^{\nu+\frac{n-1}{2}} < K^{\nu+\frac{n}{2}}.$$

Tomando esta suma como la suma de los coeficientes de la correspondiente forma modular Θ_P y aplicando la Proposición 1.6, se tendría para K suficientemente grande:

$$\sum_{k \leq K} |a_k|^2 \ll K^{\nu+\frac{n-1}{2}} = K^{\nu+\frac{n}{2}} K^{-\frac{1}{2}} \ll K^{-\frac{1}{2}} \sum_{k \leq K} |a_k|^2.$$

De aquí se concluiría que para K suficientemente grande se satisface $\sqrt{K} \ll 1$, lo cual es falso. El problema radica en que la asintótica correcta es $E_n(k,P) = \mathcal{O}(k^{-(n-3)/4})$, lo que permitiría probar el Teorema 1.10 solo para $n \geq 7$.

Es por ello que en este Capítulo, a través de formas modulares y utilizando las estimaciones adecuadas, se podrá afinar el Teorema 1.10 aplicado al grupo $\mathbf{SO}(N)$, siguiendo un método diferente al empleado por Morris y Taheri y cuyas ideas utilizadas podrían extenderse al resto de grupos.

[4] Para todo espacio vectorial V y endomorfismo f se verifica que $\dim \ker(f) + \dim \mathrm{im}(f) = \dim V$. Se emplea esta fórmula para $f = \Delta$ y $V = \mathcal{P}_n^g$, siendo $\ker(\Delta) = \mathcal{H}_n^g$ y $\mathrm{im}(\Delta) \subseteq \mathcal{P}_n^{g-2}$.

[5] Si $V \perp W$, se verifica que $\dim(V+W) = \dim V + \dim W$. Teniendo en cuenta que si $V, W \subseteq U$ entonces $V + W \subseteq U$, basta emplear la fórmula para $V = \mathcal{H}_n^g$, $W = \|\vec{x}\|^2 \mathcal{P}_n^{g-2} \subseteq (\mathcal{H}_n^g)^\perp$ y $U = \mathcal{P}_n^g$.

§2. La Ley de Weyl en $\mathbf{SO}(N)$ para $N \geq 8$

A. Paso 1 - Expresión para $\mathcal{N}(\lambda)$. Para los grupos de Lie clásicos considerados como variedades Riemannianas, la deducción de las fórmulas de los autovalores del operador $-\Delta_g$ definido sobre ellos no es una cuestión sencilla (véase [**?**] para el fundamento de la deducción de tales fórmulas). En el caso del grupo $\mathbf{SO}(N)$, de dimensión $d = N(N-1)/2$ y rango $n = N/2$ si N es par y $n = (N-1)/2$ si N es impar, los mismos aparecen indexados a través de las tuplas $\vec{b} \in \mathbb{Z}^n$ tales que $b_1 \geq \ldots \geq b_{n-1} \geq |b_n| \geq 0$ si $N = 2n$ y $b_1 \geq \ldots \geq b_n \geq 0$ si $N = 2n+1$. Partiendo de la notación que Morris y Taheri siguen en [**?**], cada elección concreta de $\vec{b}$ origina el autovalor $\lambda_{\vec{b}}$ con su correspondiente multiplicidad $m_{\vec{b}}$:

$$\lambda_{\vec{b}} = \sum_{j=1}^{n} b_j(b_j + 2a_j), \qquad m_{\vec{b}} = m_N \prod_{1 \leq i < j \leq n} \left(\frac{(b_i + a_i)^2 - (b_j + a_j)^2}{a_i^2 - a_j^2} \right)^2,$$

donde:

$$a_j = \begin{cases} n - j & \text{si } N = 2n, \\ n - j + \frac{1}{2} & \text{si } N = 2n+1; \end{cases} \qquad m_N = \begin{cases} 1 & \text{si } N = 2n, \\ \displaystyle\prod_{i=1}^{n} \left(\frac{b_i + a_i}{a_i} \right)^2 & \text{si } N = 2n+1. \end{cases}$$

Las fórmulas así presentadas son muy poco manejables, por lo que se introducen unos pequeños cambios que darán una mejor caracterización a la hora de hacer cálculos. Escribiendo $x_j = b_j + a_j$ si $N = 2n$ y $x_j = 2b_j + 2a_j$ si $N = 2n+1$, despejando b_j y sustituyendo en cada caso, se obtiene:

$$\boxed{N = 2n}$$

$$\lambda_{\vec{b}} = \sum_{j=1}^{n} (x_j + n - j)(x_j - n + j) = \sum_{j=1}^{n} x_j^2 - \sum_{j=1}^{n} j^2 = \sum_{j=1}^{n} x_j^2 - \frac{n(n-1)(2n-1)}{6},$$

$$m_{\vec{b}} = \prod_{1 \leq i < j \leq n} \left(\frac{x_i^2 - x_j^2}{(n-i)^2 - (n-j)^2} \right)^2 = \left(\prod_{i=0}^{n-1} \prod_{j=i+1}^{n-1} \frac{x_{n-j}^2 - x_{n-i}^2}{j^2 - i^2} \right)^2;$$

$$\boxed{N = 2n+1}$$

$$\lambda_{\vec{b}} = \sum_{j=1}^{n} \left(\frac{x_j - 2n - 1 + 2j}{2} \right) \left(\frac{x_j + 2n + 1 - 2j}{2} \right) = \frac{1}{4} \sum_{j=1}^{n} x_j^2 - \sum_{j=1}^{n} (j^2 + j) - \frac{n}{4} = \frac{1}{4} \sum_{j=1}^{n} x_j^2 - \frac{n(4n^2-1)}{12},$$

$$m_{\vec{b}} = \prod_{i=1}^{n} \left(\frac{x_i}{2n+1-2j} \right)^2 \prod_{1 \leq i < j \leq n} \left(\frac{x_i^2 - x_j^2}{(2n+1-2i)^2 - (2n+1-2j)^2} \right)^2$$

$$= \left(\prod_{i=0}^{n-1} \frac{x_{n-i}}{2i+1} \prod_{j=i+1}^{n-1} \frac{x_{n-j}^2 - x_{n-i}^2}{(2j+1)^2 - (2i+1)^2} \right)^2;$$

donde en las expresiones de $m_{\vec{b}}$, el producto interior es 1 cuando $i = n-1$. Una vez que las fórmulas tienen este aspecto es posible expresar también la función $\mathcal{N}(\lambda)$ de una forma más adecuada:

Lema 1.11 *Sea $m_N(\vec{x}) := m_{\vec{b}}$. Tomando $\chi_R := \chi_{\mathbb{B}_R^n}$, se tiene para ciertas constantes $C_{1,N}$ y R_N:*

$$\mathcal{N}(\lambda) = C_{1,N} \sum_{\vec{x} \in \mathbb{A}^n} m_N(\vec{x}) \chi_{R_N}(\vec{x}),$$

donde $\mathbb{A} = \mathbb{Z}$ si $N = 2n$ y $\mathbb{A} = \mathbb{O} = 2\mathbb{Z} + 1$ si $N = 2n+1$.

Demostración. Puesto que las expresiones para los autovalores y sus multiplicidades han sido transformadas en función de los vectores $\vec{x}$, se realiza lo mismo para su indexado. Si $N = 2n$, $b_1 \geq \ldots \geq b_{n-1} \geq |b_n| \geq 0$ y $\vec{b} \in \mathbb{Z}^n$ es equivalente a que $x_1 - (n-1) \geq \ldots \geq x_{n-1} - (n-(n-1)) \geq |x_n - (n-n)| \geq 0$ y $\vec{x} \in \mathbb{Z}^n$. Para cada $i = 1, \ldots, n-2$ se tiene que $x_i - (n-i) \geq x_{i+1} - (n-(i+1))$, es decir, $x_i > x_{i+1}$; mientras que para $i = n-1$ se tiene que $x_{n-1} - 1 \geq |x_n|$, es decir, $x_{n-1} > |x_n|$. Por tanto, para $N = 2n$ el indexado se transforma

en $x_1 > \ldots > x_{n-1} > |x_n| \geq 0$ con $\vec{x} \in \mathbb{Z}^n$. Por otra parte, si $N = 2n+1$, $b_1 \geq \ldots \geq b_{n-1} \geq b_n \geq 0$ y $\vec{b} \in \mathbb{Z}^n$ es equivalente a que $x_1 - (2n+1-2) \geq \ldots \geq x_n - (2n+1-2n) \geq 0$ y $\vec{x} \in \mathbb{O}^n$. Para cada $i = 1, \ldots, n-1$ se tiene que $x_i - (2n+1-2i) \geq x_{i+1} - (2n+1-2(i+1))$, es decir, $x_i - 2 \geq x_{i+1}$ y así $x_i > x_{i+1}$ (ya que $x_i \in \mathbb{O}$); mientras que para $i = n$ se tiene que $x_n - 1 \geq 0$, es decir, $x_n > 0$. Por tanto, para $N = 2n+1$ el indexado se transforma en $x_1 > \ldots > x_n > 0$ con $\vec{x} \in \mathbb{O}^n$. Los nuevos indexados obtenidos se denotarán por $C_{\mathbb{A}}$, siendo $C_{\mathbb{Z}} = \{\vec{x} \in \mathbb{Z}^n : x_1 > \ldots > x_{n-1} > |x_n| \geq 0\}$ en el caso $N = 2n$ y $C_{\mathbb{O}} = \{\vec{x} \in \mathbb{O}^n : x_1 > \ldots > x_n > 0\}$ en el caso $N = 2n+1$. Al margen de los indexados ya transformados, utilizando la nueva expresión calculada para $\lambda_{\vec{b}}$, se verifica directamente que $\lambda_{\vec{b}} \leq \lambda$ si y solo si:

$$\sum_{j=1}^{n} x_j^2 = \|x\|^2 \leq R_N := \begin{cases} \lambda + \dfrac{n(n-1)(2n-1)}{6} & \text{si } N = 2n, \\ 4\lambda + \dfrac{n(4n^2-1)}{3} & \text{si } N = 2n+1. \end{cases}$$

Por otra parte, el polinomio que define la multiplicidad $m_N(\vec{x})$ es invariante por construcción bajo cambios de signo y de orden entre las variables x_i y se anula cuando al menos dos de las variables son iguales. Esto posibilita que tomar los $\vec{x} \in C_{\mathbb{A}}$ sea equivalente a tomar todos los $\vec{x} \in \mathbb{A}^n$ para evaluar $\mathcal{N}(\lambda)$ dividiendo por los $n!$ posibles cambios de orden y los 2^{n-1} o 2^n (según el caso) cambios de signo para las variables x_i. Tomando las constantes $C_{1,N} := 1/(2^{n-1}n!)$ si $N = 2n$ y $C_{1,N} := 1/(2^n n!)$ si $N = 2n+1$ y teniendo en cuenta todas las transformaciones, se concluye:

$$\mathcal{N}(\lambda) = \sum_{\lambda_{\vec{b}} \leq \lambda} 1 = \sum_{\substack{\vec{x} \in C_{\mathbb{A}} \\ \|\vec{x}\|^2 \leq R_N}} 1 = \sum_{\vec{x} \in C_{\mathbb{A}}} m_N(\vec{x}) \chi_{R_N}(\vec{x}) = C_{1,N} \sum_{\vec{x} \in \mathbb{A}^n} m_N \chi_{R_N}(\vec{x}).$$

□

Puesto que el polinomio $m_N(\vec{x})$ es homogéneo, el siguiente paso es aplicar la Proposición 1.9. Para ello se calcula en primer lugar el grado de $m_N(\vec{x})$. En el caso $N = 2n$, cada $0 \leq i \leq n-1$ aporta al grado la cantidad $2 \cdot 2 \cdot (n-i-1)$, mientras que en el caso $N = 2n+1$, cada $0 \leq i \leq n-1$ aporta al grado la cantidad $2 \cdot (2 \cdot (n-i-1)+1)$. Por tanto:

$$\deg(m_N(\vec{x})) = \begin{cases} 4 \displaystyle\sum_{j=1}^{n-1} j = 2n(n-1) & \text{si } N = 2n; \\ 2 \cdot \left(2 \displaystyle\sum_{j=0}^{n-1} j + n \right) = 2n^2 & \text{si } N = 2n+1. \end{cases}$$

Puesto que $\dim(\mathbf{SO}(2n)) = n(2n-1)$ y $\dim(\mathbf{SO}(2n+1)) = n(2n+1)$, se puede concluir de manera uniforme que si $d = \dim(\mathbf{SO}(N))$, entonces $\deg(m_N(\vec{x})) = d - n$ y es un número par. Aplicando entonces la Proposición 1.9:

$$m_N(\vec{x}) = \sum_{l=0}^{\frac{d-n}{2}} \|\vec{x}\|^{2l} P_{d-n-2l}(\vec{x}).$$

Si se sustituye esta descomposición en la fórmula de $\mathcal{N}(\lambda)$ y se separa la contribución del polinomio armónico constante P_0, se tiene:

$$\begin{aligned} \mathcal{N}(\lambda) &= C_{1,N} \sum_{\vec{x} \in \mathbb{A}^n} \sum_{l=0}^{\frac{d-n}{2}} \|\vec{x}\|^{2l} P_{d-n-2l}(\vec{x}) \chi_{R_N}(\vec{x}) \\ &= C_{1,N} P_0 \sum_{\vec{x} \in \mathbb{A}^n} \|\vec{x}\|^{d-n} \chi_{R_N}(\vec{x}) + C_{1,N} \sum_{\vec{x} \in \mathbb{A}^n} \sum_{l=0}^{\frac{d-n}{2}-1} \|\vec{x}\|^{2l} P_{d-n-2l}(\vec{x}) \chi_{R_N}(\vec{x}). \end{aligned}$$

La suma en los polinomios P_j es finita, por lo que existe un índice l_0 que da el máximo de las sumas en todas las tuplas $\vec{x} \in \mathbb{A}$, es decir, para todo $l = 0, 1, \ldots, (d-n)/2 - 1$ se verifica:

$$\left| \sum_{\vec{x} \in \mathbb{A}^n} \|\vec{x}\|^{2l} P_{d-n-2l}(\vec{x}) \chi_{R_N}(\vec{x}) \right| \leq \left| \sum_{\vec{x} \in \mathbb{A}^n} \|\vec{x}\|^{2l_0} P_{d-n-2l_0}(\vec{x}) \chi_{R_N}(\vec{x}) \right|.$$

Escribiendo $\nu = d - n - 2l_0$, se concluye que existe $0 < \nu \leq d - n$ tal que $\mathcal{N}(\lambda)$ satisface la expresión:

$$\mathcal{N}(\lambda) = C_{1,N} P_0 \sum_{\vec{x} \in \mathbb{A}^n} \|\vec{x}\|^{d-n} \chi_{R_N}(\vec{x}) + \mathcal{O}\left(\sum_{\vec{x} \in \mathbb{A}^n} \|\vec{x}\|^{d-n-\nu} P_\nu(\vec{x}) \chi_{R_N}(\vec{x}) \right).$$

B. Paso 2 - Aplicación de las formas modulares. Realizando el cambio de variable $\|\vec{x}\|^2 = k$ en la expresión que se ha obtenido para $\mathcal{N}(\lambda)$, se cumple que $\{\vec{x} \in \mathbb{A}^n \,:\, \|\vec{x}\|^2 = k\} = r_n^{\mathbb{A}}(k)$ y si $\vec{x} \in \mathbb{B}^n_{R_N}$, entonces $k \leq R_N^2$. Con esto es posible deducir que el término principal de $\mathcal{N}(\lambda)$ satisface:

$$C_{1,N} P_0 \sum_{\vec{x} \in \mathbb{A}^n} \|\vec{x}\|^{d-n} \chi_{R_N}(\vec{x}) = C_{1,N} P_0 \sum_{k \leq R_N^2} k^{\frac{d-n}{2}} r_n^{\mathbb{A}}(k).$$

En cuanto al término de error, sin embargo, será donde se apliquen las formas modulares. Para poder hacerlo, hay que realizar la sumación en $\mathbb{Z}$, por lo que se debe transformar la suma en $\mathbb{O}$ del caso impar. De forma genérica se tendría, si se toma $\mathbb{E} := 2\mathbb{Z}$:

$$\sum_{\vec{x} \in \mathbb{O}^n} f(x_1, \ldots, x_n) = \sum_{\vec{x} \in \mathbb{Z}^n} f(x_1, \ldots, x_n) - \sum_{1 \leq i \leq n} \sum_{\substack{\vec{x} \in \mathbb{Z}^n \\ x_i \in \mathbb{E}}} f(x_1, \ldots, x_n) + \sum_{1 \leq i < j \leq n} \sum_{\substack{\vec{x} \in \mathbb{Z}^n \\ x_i,\, x_j \in \mathbb{E}}} f(x_1, \ldots, x_n)$$

$$- \ldots + (-1)^n \sum_{\vec{x} \in \mathbb{E}^n} f(x_1, \ldots, x_n) = \sum_{\vec{x} \in \mathbb{Z}^n} f(x_1, \ldots, x_n) - \sum_{1 \leq i \leq n} \sum_{\vec{x} \in \mathbb{Z}^n} f(x_1, \ldots, 2x_i, \ldots, x_n)$$

$$+ \sum_{1 \leq i < j \leq n} \sum_{\vec{x} \in \mathbb{Z}^n} f(x_1, \ldots, 2x_i, \ldots, 2x_j, \ldots, x_n) - \ldots + (-1)^n \sum_{\vec{x} \in \mathbb{Z}^n} f(2x_1, \ldots, 2x_n).$$

Gracias a esta deducción, la suma del término de error de $\mathcal{N}(\lambda)$ queda en cada caso $N = 2n$ y $N = 2n + 1$, respectivamente:

$$\sum_{\vec{x} \in \mathbb{Z}^n} \|I_{n\times n}\vec{x}\|^{d-n-\nu} P_\nu(I_{n\times n}\vec{x}) \chi_{R_N}(I_{n\times n}\vec{x}), \qquad \sum_{J \subseteq \{1,\ldots,n\}} (-1)^{|J|} \sum_{\vec{x} \in \mathbb{Z}^n} \|T_J\vec{x}\|^{d-n-\nu} P_\nu(T_J\vec{x}) \chi_{R_N}(T_J\vec{x}),$$

donde, $I_{n\times n}$ es la matriz identidad y $T_J = \mathrm{diag}(1 + \delta_J(j))_{n\times n}$, siendo $\delta_J(j)$ la función que vale 1 si $j \in J$ y 0 en otro caso. Denotando a cada matriz por M y escribiendo $k = Q(\vec{x}) := \|M\vec{x}\|^2$, se verifica:

$$P_\nu(M\vec{x}) = \|M\vec{x}\|^\nu P_\nu\left(\frac{M\vec{x}}{\|M\vec{x}\|}\right) = k^{\frac{\nu}{2}} (P_\nu \circ M)\left(\frac{\vec{x}}{\sqrt{k}}\right)$$

Si se toma ahora $P_{\nu,M} := P_\nu \circ M$, la suma en las tuplas $\vec{x} \in \mathbb{Z}^n$ cumple:

$$\sum_{\vec{x} \in \mathbb{Z}^n} \|M\vec{x}\|^{d-n-\nu} P_\nu(M\vec{x}) \chi_{R_N}(M\vec{x}) = \sum_{k \leq R_N^2} k^{\frac{d-n-\nu}{2}} k^{\frac{\nu}{2}} \sum_{\|M\vec{x}\|^2 = k} P_{\nu,M}\left(\frac{\vec{x}}{\sqrt{k}}\right) = \sum_{k \leq R_N^2} k^{\frac{d-n}{2}} r_n^Q(k, P_{\nu,M}).$$

Para cada una de las matrices M, sean $k^{\nu/2} r_n^Q(k, P_{\nu,M})$ los coeficientes de Fourier de la correspondiente función theta:

$$\Theta_{P_{\nu,M}}(z) = \sum_{k=1}^{\infty} k^{\frac{\nu}{2}} r_n^Q(k, P_{\nu,M}) e^{2\pi i k z}.$$

Según la formulación de las funciones theta, al ser $\frac{1}{2}A[\vec{m}] = Q(\vec{m}) = \|M\vec{m}\|^2 = \vec{m}^t M^t M \vec{m}$, entonces cada polinomio $P_{\nu,M}$ es esférico con respecto a la correspondiente matriz $A = 2M^tM = 2M^2$. En efecto, $A = 2I_{n\times n}$ en el caso $N = 2n$ o bien $A = \mathrm{diag}(a_j)_{n\times n}$ con $a_j = 2 + 6\delta_J(j)$ para cada $J \subseteq \{1, \ldots, n\}$ en el caso $N = 2n + 1$. En todos los casos A es definida positiva y al ser diagonal, $A^{-1} = \mathrm{diag}(a_j^{-1})$ y para $N_0 = 4$ en el caso $N = 2n$ y $N_0 = 16$ en el caso $N = 2n + 1$, las matrices $N_0 A^{-1}$ y A tienen entradas pares. Por otra parte, $P_{\nu,M}$ es de grado par $\nu > 0$, ya que provenía de una descomposición en armónicos que por construcción solo contenía grados pares. Basta ver que siendo P_ν armónico, entonces $P_{\nu,M}$ es esférico sobre A. Realizando el cambio de variable $\vec{y} = M\vec{x}$:

$$A\left[\frac{\partial}{\partial \vec{x}}\right] P_{\nu,M} = \frac{1}{2}\left(\frac{\partial}{\partial \vec{x}}\right)^t M^{-1} M^{-1} \frac{\partial}{\partial \vec{x}} (P_\nu(M\vec{x})) = \frac{1}{2}\left(\frac{\partial}{\partial \vec{y}}\right)^t \frac{\partial}{\partial \vec{y}} (P_\nu(\vec{y})) = \frac{1}{2}\Delta P_\nu(\vec{y}) = 0.$$

Aplicando el Teorema 1.8, $\Theta_{P_{\nu,M}}$ es una forma cuspidal de peso $\nu + n/2$ para $\Gamma_0(8)$ en el caso $N = 2n$ y $\Gamma_0(32)$ en el caso $N = 2n + 1$. De esta manera, se puede utilizar la Proposición 1.5 para llegar a:

$$\sum_{k \leq R_N^2} k^{\frac{\nu}{2}} r_n^Q(k, P_{\nu,M}) = \mathcal{O}\left(R_N^{\nu + \frac{n}{2}} \log R_N\right).$$

En consecuencia, el término de error de $\mathcal{N}(\lambda)$ verifica en todos los casos:

$$\mathcal{O}\left(\sum_{\vec{x}\in\mathbb{A}^n}\|\vec{x}\|^{d-n-\nu}\,P_\nu(\vec{x})\chi_{R_N}(\vec{x})\right)=\mathcal{O}\left(\sum_{k\leq R_N^2}k^{\frac{d-n-\nu}{2}}k^{\frac{\nu}{2}}r_n^Q(k,P_{\nu,M})\right),$$

y teniendo en cuenta lo que se acaba de probar a través de las formas modulares, se puede emplear (14) tomando $a_k=k^{\nu/2}r_n^Q(k,P_{\nu,M})$ y $f(k)=k^{(d-n-\nu)/2}$ para deducir:

$$\sum_{k\leq R_N^2}k^{\frac{d-n}{2}}r_n^Q(k,P_{\nu,M})=\mathcal{O}\left(R_N^{d-\frac{n}{2}}\log R_N\right)+\mathcal{O}\left(\int_1^{R_N^2}t^{\frac{d}{2}-\frac{n}{4}-1}\log t\,dt\right)=\mathcal{O}\left(R_N^{d-\frac{n}{2}}\log R_N\right).$$

En conclusión, la fórmula asintótica para $\mathcal{N}(\lambda)$ queda, tras todas las modificaciones anteriores:

$$\mathcal{N}(\lambda)=C_{1,N}P_0\sum_{k\leq R_N^2}k^{\frac{d-n}{2}}r_n^{\mathbb{A}}(k)+\mathcal{O}\left(R_N^{d-\frac{n}{2}}\log R_N\right).$$

C. Paso 3 - Fórmulas para $r_n^{\mathbb{A}}$. El siguiente paso en el análisis de $\mathcal{N}(\lambda)$ es descubrir una fórmula para $r_n^{\mathbb{A}}(k)$, es decir, para el número de representaciones de k como suma de n cuadrados en $\mathbb{A}$. Visto de esta forma, una fórmula para los casos $\mathbb{Z}$ y $\mathbb{O}$ ya se ha probado cuando $n=4$ y es conocida como el *Teorema de los cuatro cuadrados de Jacobi*. Una prueba clásica de ello puede consultarse en [**?**], donde se hace referencia al comportamiento de un tipo particular de unas funciones especiales llamadas *funciones elípticas*. Sin embargo, la notación empleada hace necesario entender previamente todos los parámetros involucrados. A continuación se expone un resultado previo que evitará apelar a ningún conocimiento profundo sobre funciones elípticas y del que se podrá deducir directamente el *Teorema de los cuatro cuadrados de Jacobi*. La base de dicho resultado es notar que si $f(z)$ es una función entera y periódica de períodos independientes 1 y τ con $\mathrm{Im}(\tau)>0$, entonces por el *Teorema de Liouville*, $f(z)$ es constante. Teniendo esto en cuenta, se puede probar:

Lema 1.12 *Las funciones holomorfas en $|w|<1$:*

$$F_1(w):=\sum_{n=1}^{\infty}\frac{(2n-1)w^{2n-1}}{1-w^{4n-2}},\qquad G_1(w):=\sum_{n=0}^{\infty}w^{(2n+1)^2},$$

$$F_2(w):=1+8\left(\sum_{n=1}^{\infty}\frac{(2n-1)w^{2n-1}}{1-w^{2n-1}}+\sum_{n=1}^{\infty}\frac{2nw^{2n}}{1+w^{2n}}\right),\qquad G_2(w):=1+2\sum_{n=1}^{\infty}w^{(2n)^2}$$

verifican las identidades $F_i(w^4)=(G_i(w))^4$ respectivamente para $i=1,2$.

Demostración. Sea la función para τ tal que $\mathrm{Im}(\tau)>0$:

$$\theta(z,\tau)=\sum_{n=-\infty}^{\infty}q^{n^2}e^{2\pi inz},\qquad q:=e^{i\pi\tau}.$$

Gracias a que $\mathrm{Im}(\tau)>0$, los coeficientes q^{n^2} de la serie tienden a cero exponencialmente y así la serie define una función entera. A lo largo de la prueba, se convendrá en que $\theta(z,\tau)=\theta(z)$, dejando τ (y en consecuencia q) como parámetro constante y especificando su variabilidad cuando sea necesario. Por definición de $\theta(z)$ se verifican las propiedades:

$$\theta(z+1)=\theta(z),\qquad \theta(z+\tau)=q^{-1}e^{-2\pi iz}\theta(z).$$

Puesto que resulta conveniente trabajar con funciones que sean doblemente periódicas ($\theta(z)$ casi lo es), se toman los cocientes:

$$A(z):=\frac{e^{-\pi iz}\theta(z+1/2)}{\theta(z+\omega)},\qquad B_1(z):=\frac{e^{-\pi iz}\theta(z)}{\theta(z+\omega)},\qquad B_2(z):=\frac{\theta(z+\tau/2)}{\theta(z+\omega)}.$$

Estos cocientes cumplen en general $f(z+1)=\pm f(z)$ y $f(z+\tau)=\pm f(z)$, por lo que $A^2(z)$ y $B_i^2(z)$ son funciones *elípticas*, es decir, meromorfas con períodos 1 y τ, pero no son enteras ya que en principio, su denominador puede anularse. Además, modificando ligeramente la serie de $\theta(z)$, se ve que las funciones $A(z)$ y $B_i(z)$ son impares gracias a las relaciones:

$$\theta(z)=\theta(-z),\qquad \theta\left(z+\frac{1}{2}\right)=\theta\left(\frac{1}{2}-z\right),\qquad \theta\left(z+\frac{\tau}{2}\right)=e^{-2\pi iz}\theta\left(\frac{\tau}{2}-z\right),\qquad \theta(z+\omega)=-e^{-2\pi iz}\theta(\omega-z).$$

En consecuencia, $A^2(z)$ y $B_i^2(z)$ son funciones pares y de la última relación para $z=0$ es posible deducir que $\theta(\omega)=0$ y por la periodicidad, todo $z=\omega+n+m\tau$ con $n,m\in\mathbb{Z}$ verifica $\theta(z)=0$. Por otra parte, las combinaciones $\theta^2(0)A^2(z)-\theta^2(1/2)B_1^2(z)$ y $\theta^2(\tau/2)A^2(z)-\theta^2(1/2)e^{2\pi iz}B_2^2(z)$ cancelan el polo doble en $z=0$ y por periodicidad y al ser $A^2(z)$ y $B_i^2(z)$ pares, cancelan todos los polos posibles. Por tanto, ambas combinaciones definen funciones enteras y aplicando el *Teorema de Liouville*:

$$\frac{e^{-2\pi iz}\left(\theta^2(0)\theta^2(z+1/2)-\theta^2(1/2)\theta^2(z)\right)}{\theta^2(z+\omega)}=K_1,\qquad \frac{e^{-2\pi iz}\theta^2(\tau/2)\theta^2(z+1/2)-\theta^2(1/2)e^{2\pi iz}\theta^2(z+\tau/2)}{\theta^2(z+\omega)}=K_2,$$

donde K_1 y K_2 son constantes (diferentes para cada elección de τ). Tomando respectivamente $z=\omega$ y $z=1/2$ se sigue que $K_1=-q\theta^2(\tau/2)$ y $K_2=-\theta^2(0)$. Por otra parte, puesto que $\theta(z)$, $\theta(z+1/2)$ y $L(z):=e^{\pi iz}\theta(z+\tau/2)$ son funciones pares, en un entorno de $z=0$ satisfacen un desarrollo del tipo $f(z)=f(0)+f''(0)z^2/2+\ldots$ De esta forma, al sustituir f por cada una de ellas y sustituir sus desarrollos en la expresión de cada K_i, se obtiene cuando $z\to 0$:

$$K_1=\frac{\theta(0)\theta(1/2)}{(\theta'(\omega))^2}\left(\theta(0)\theta''(1/2)-\theta(1/2)\theta''(0)\right),\qquad K_2=\frac{\theta(\tau/2)\theta(1/2)}{(\theta'(\omega))^2}\left(\theta(\tau/2)\theta''(1/2)-\theta(1/2)L''(0)\right).$$

Al igualar las dos fórmulas conseguidas para cada K_i, se concluyen las identidades:

$$\frac{\theta''(0)}{\theta(0)}-\frac{\theta''(1/2)}{\theta(1/2)}=q\left(\frac{\theta(\tau/2)\theta'(\omega)}{\theta(1/2)\theta(0)}\right)^2,\qquad \frac{\theta''(1/2)}{\theta(1/2)}-\frac{L''(0)}{L(0)}=\left(\frac{\theta(0)\theta'(\omega)}{\theta(\tau/2)\theta(1/2)}\right)^2.$$

Para poder simplificar estas identidades se recurre a una formulación alternativa para $\theta(z)$. Sea el producto infinito:

$$P(z)=\prod_{n=1}^{\infty}\left(1+q^{2n-1}e^{2\pi iz}\right)\left(1+q^{2n-1}e^{-2\pi iz}\right).$$

Esta función también satisface las propiedades $P(z+1)=P(z)$ y $P(z+\tau)=q^{-1}e^{-2\pi iz}P(z)$. Dada la similitud existente entre $\theta(z)$ y $P(z)$, el cociente $\theta(z)/P(z)$ es una función elíptica. Además, cada cero de $\theta(z)$ de la forma $z=\omega+n+m\tau$ anula un factor de P y cada factor de P se anula en uno de dichos ceros. De nuevo por el *Teorema de Liouville*, $\theta(z)/P(z)=C$ constante [6](diferente según el valor τ). Para hallar C, se sustituye $z=1/2$ y $z=1/4$ respectivamente en su expresión, por lo que:

$$\frac{C}{\prod(1-q^{2n})}=\frac{\sum(-1)^n q^{n^2}}{\prod(1-q^{2n-1})^2(1-q^{2n})}=\frac{\sum(-1)^n q^{4n^2}}{\prod(1+q^{4n-2})(1-q^{2n})}.$$

Si en el denominador de la segunda fracción se cambia q por q^4 se deduce:

$$\prod_{n=1}^{\infty}\left(1-q^{8n-4}\right)^2\left(1-q^{8n}\right)=\prod_{n=1}^{\infty}\left(1+q^{4n-2}\right)\prod_{n=1}^{\infty}\left(1-q^{4n-2}\right)\left(1-q^{8n-4}\right)\left(1-q^{8n}\right)=\prod_{n=1}^{\infty}\left(1+q^{4n-2}\right)\left(1-q^{2n}\right),$$

ya que todo número par puede expresarse sin ambigüedad como o bien $4n-2$ o bien $8n-4$ o bien $8n$. Así se recupera el denominador de la tercera fracción y la segunda fracción define una función $f(q)$ holomorfa en $|q|<1$ que cumple $f(q)=f(q^4)$. Al observar su desarrollo de Taylor en $q=0$ verifica $f(q)=f(0)=1$ y con esto se llega a:

$$C=\prod_{n=1}^{\infty}(1-q^{2n}).$$

Sustituyendo se obtiene la famosa *Fórmula del triple producto de Jacobi*:

$$\theta(z)=\prod_{n=1}^{\infty}\left(1-q^{2n}\right)\left(1+q^{2n-1}e^{2\pi iz}\right)\left(1+q^{2n-1}e^{-2\pi iz}\right).$$

Gracias a esta fórmula, se pueden realizar grandes simplificaciones en las identidades requeridas tal y como se buscaba. Derivando la fórmula se sigue:

$$\theta'(z)=C\sum_{n=1}^{\infty}\left[2\pi iq^{2n-1}\left(e^{2\pi iz}-e^{-2\pi iz}\right)\right]\prod_{m\neq n}\left(1+q^{2m-1}e^{2\pi iz}\right)\left(1+q^{2m-1}e^{-2\pi iz}\right).$$

[6] Esto implica que si $\theta(z)=0$ entonces $z=\omega+n+m\tau$ con $n,m\in\mathbb{Z}$, ya que si hubiera otros ceros o alguno fuese doble, entonces $C=0$, lo cual es imposible al ser $\theta(z)$ no idénticamente nula. Como anteriormente se ha probado la implicación inversa, se tiene la equivalencia y los únicos ceros de $\theta(z)$ son de la forma $z=\omega+n+m\tau$ con $n,m\in\mathbb{Z}$.

Con ambas fórmulas presentes, se calculan directamente los valores:

$$\theta(0) = C\prod_{n=1}^{\infty}\left(1+q^{2n-1}\right)^2, \qquad \theta\left(\frac{1}{2}\right) = C\prod_{n=1}^{\infty}\left(1-q^{2n-1}\right)^2, \qquad \theta\left(\frac{\tau}{2}\right) = 2C\prod_{n=1}^{\infty}\left(1+q^{2n}\right)^2, \qquad \theta'(\omega) = 2\pi i C^3.$$

Con estos valores se deduce:

$$\frac{\pi i\theta(0)\theta(1/2)\theta(\tau/2)}{\theta'(\omega)} = \prod_{n=1}^{\infty}\left(1-q^{4n-2}\right)^2\left(1+q^{2n}\right)^2 = \prod_{n=1}^{\infty}\frac{(1-q^{4n-2})^2(1-q^{4n})^2}{(1-q^{2n})^2} = 1.$$

Utilizando convenientemente este cociente, el segundo miembro de cada una de las identidades referidas queda, dividendo entre $-\pi^2$ en la primera y entre π^2 en la segunda:

$$-\frac{q}{\pi^2}\left(\frac{\theta(\tau/2)\theta'(\omega)}{\theta(1/2)\theta(0)}\right)^2 = q\theta^4\left(\frac{\tau}{2}\right) = \left(\sum_{n=-\infty}^{\infty} q^{(n+1/2)^4}\right)^4 = \left(2\sum_{n=0}^{\infty} q^{(n+1/2)^4}\right)^4 = 16\left(G_1(w)\right)^4,$$

$$\frac{1}{\pi^2}\left(\frac{\theta(0)\theta'(\omega)}{\theta(\tau/2)\theta(1/2)}\right)^2 = \theta^4(0) = \left(\sum_{n=-\infty}^{\infty} q^{n^2}\right)^4 = \left(G_2(w)\right)^4,$$

donde $w = q^{1/4}$. Para finalizar, considerando q como variable y derivando las series de $\theta(z)$ y $L(z)$ tanto respecto de z como de q, se verifican las relaciones:

$$\theta''(z) = -4\pi^2\sum_{n=-\infty}^{\infty} n^2 q^{n^2} e^{2\pi i n z} = -4\pi^2 q\frac{\partial\theta(z)}{\partial q},$$

$$L''(z) = -\pi^2\sum_{n=-\infty}^{\infty}(2n+1)^2 q^{n^2+n} e^{(2n+1)\pi i z} = -4\pi^2 q^{\frac{3}{4}}\frac{\partial}{\partial q}\left(q^{\frac{1}{4}}L(z)\right),$$

por lo que al emplearlas para los valores correspondientes en el primer miembro de cada una de las identidades referidas queda, de nuevo dividiendo entre $-\pi^2$ la primera y entre π^2 la segunda:

$$\begin{aligned}-\frac{1}{\pi^2}\left(\frac{\theta''(0)}{\theta(0)} - \frac{\theta''(1/2)}{\theta(1/2)}\right) &= 4q\frac{\partial}{\partial q}\left(\log\frac{\theta(0)}{\theta(1/2)}\right) = 4q\frac{\partial}{\partial q}\left(\log\prod_{n=1}^{\infty}\frac{(1+q^{2n-1})^2}{(1-q^{2n-1})^2}\right)\\ &= 4q\sum_{n=1}^{\infty}\frac{\partial}{\partial q}\left(\log\frac{(1+q^{2n-1})^2}{(1-q^{2n-1})^2}\right) = 16\sum_{n=1}^{\infty}\frac{(2n-1)q^{2n-1}}{1-q^{4n-2}} = 16F_1(w^4),\end{aligned}$$

$$\begin{aligned}\frac{1}{\pi^2}\left(\frac{\theta''(1/2)}{\theta(1/2)} - \frac{L''(0)}{L(0)}\right) &= -4q\frac{\partial}{\partial q}\left(\log\frac{\theta(1/2)}{q^{1/4}L(0)}\right) = -4q\frac{\partial}{\partial q}\left(\log\left(\frac{1}{2q^{1/4}}\prod_{n=1}^{\infty}\frac{(1-q^{2n-1})^2}{(1+q^{2n})^2}\right)\right)\\ &= -4q\sum_{n=1}^{\infty}\frac{\partial}{\partial q}\left(-\log\left(2q^{\frac{1}{4}}\right) + \log\frac{(1-q^{2n-1})^2}{(1+q^{2n})^2}\right) = 1 + 8\sum_{n=1}^{\infty}\frac{(2n-1)q^{2n-1}}{1-q^{2n-1}} + 8\sum_{n=1}^{\infty}\frac{2nq^{2n}}{1+q^{2n}} = F_2(w^4),\end{aligned}$$

de nuevo con $w = q^{1/4}$. Igualando ambos miembros analizados para cada identidad, se concluye el enunciado. □

Este Lema permite probar directamente el resultado buscado:

Teorema 1.13 *(Teorema de los cuatro cuadrados de Jacobi) Para $k \in \mathbb{Z}$, sea $r_4^{\mathbb{A}}(k)$ el número de representaciones de k como suma de cuatro cuadrados en $\mathbb{A}$. Entonces:*

$$r_4^{\mathbb{Z}}(k) = \begin{cases} 8\sigma(k) & \text{si } k \text{ es impar},\\ 24\sigma_{\mathbb{O}}(k) & \text{si } k \text{ es par}; \end{cases} \qquad r_4^{\mathbb{O}}(k) = \begin{cases} 16\sigma(k/4) & \text{si } 4|k,\\ 0 & \text{en otro caso.}\end{cases}$$

donde $\sigma_{\mathbb{O}}(k)$ es la función aritmética $\sigma(k)$ contando únicamente los divisores impares.

Demostración. Para concluir cada identidad basta desarrollar cada uno de los miembros de las identidades $F_i(w^4) = (G_i(w))^4$ dadas por el Lema 1.12 tomando $w = q^{1/4}$. Utilizando sumas de progresiones aritméticas se sigue:

$$F_1(w^4) = F_1(q) = \sum_{\substack{n=1\\ n\in\mathbb{O}}}^{\infty} \frac{nq^n}{1-q^{2n}} = \frac{1}{2}\sum_{\substack{n=1\\ n\in\mathbb{O}}}^{\infty} n\left(\frac{1}{1-q^n} - \frac{1}{1+q^n}\right) = \frac{1}{2}\sum_{\substack{n=1\\ n\in\mathbb{O}}}^{\infty} n\sum_{m=0}^{\infty}(q^{nm} - (-q^n)^m)$$
$$= \sum_{\substack{n=1\\ n\in\mathbb{O}}}^{\infty} n\sum_{\substack{m=1\\ m\in\mathbb{O}}}^{\infty} q^{nm} = \sum_{\substack{k=1\\ k\in\mathbb{O}}}^{\infty} q^k \sum_{d|k} d = \sum_{\substack{k=1\\ k\in\mathbb{O}}}^{\infty} \sigma(k)q^k.$$

De modo similar:

$$F_2(w^4) = F_2(q) = 1 + 16\sum_{n=1}^{\infty}\frac{nq^{2n}}{1+q^{2n}} + 8\sum_{\substack{n=1\\ n\in\mathbb{O}}}^{\infty}\frac{nq^n}{1-q^n} = 1 - 16\sum_{n=1}^{\infty} n\sum_{m=1}^{\infty}(-q^{2n})^m + 8\sum_{\substack{n=1\\ n\in\mathbb{O}}}^{\infty} n\sum_{m=1}^{\infty} q^{nm}$$
$$= 1 - 16\sum_{k=1}^{\infty} q^{2k}\sum_{d|k}(-1)^{\frac{k}{d}}d + 8\sum_{k=1}^{\infty} q^k \sum_{\substack{d|k\\ d\in\mathbb{O}}} d.$$

Sea $f(k) = -\sum_{d|k}(-1)^{k/d}d$. $f(k)$ es una función multiplicativa por (2) ya que los sumandos son funciones multiplicativas. Para calcular su valor, basta ver que si $k = 2^\nu k'$ con $k' \in \mathbb{O}$ entonces $f(k) = f(k') = \sum_{d|k'} d = \sigma(m') = \sigma_{\mathbb{O}}(k') = \sigma_{\mathbb{O}}(k)$ si $\nu = 0$, mientras que $f(k) = f(2^\nu)f(k') = -(1+2+\ldots+2^{\nu-1}-2^\nu)\sigma_{\mathbb{O}}(k') = \sigma_{\mathbb{O}}(k') = \sigma_{\mathbb{O}}(k)$ si $\nu > 0$. Por tanto, en ambos casos $f(k) = \sigma_{\mathbb{O}}(k)$, por lo que:

$$F_2(w^4) = 1 + 16\sum_{k=1}^{\infty}\sigma_{\mathbb{O}}(k)q^{2k} + 8\sum_{k=1}^{\infty}\sigma_{\mathbb{O}}(k)q^k.$$

Por otra parte, expresando explícitamente G_1:

$$(G_1(w))^4 = \left(\sum_{n=0}^{\infty} q^{(n+1/2)^2}\right)^4 = \left(\sum_{\substack{n=1\\ n\in\mathbb{O}}}^{\infty} q^{n^2/4}\right)^4 = \sum_{\substack{n_1,n_2,n_3,n_4\in\mathbb{O}\\ n_j\geq 1}} q^{(n_1^2+n_2^2+n_3^2+n_4^2)/4}$$
$$= \frac{1}{16}\sum_{k=1}^{\infty} q^k \sum_{\substack{n_1^2+n_2^2+n_3^2+n_4^2=4k\\ n_j\in\mathbb{O}}} 1 = \frac{1}{16}\sum_{k=1}^{\infty} r_4^{\mathbb{O}}(4k)q^k = \frac{1}{16}\sum_{\substack{k=1\\ k\in\mathbb{O}}}^{\infty} r_4^{\mathbb{O}}(k)q^k,$$

siendo cierta la última igualdad debido a que si $n = n_1^2+n_2^2+n_3^2+n_4^2$ con $n_j \in \mathbb{O}$, entonces n puede expresarse como $4k$ con $k \in \mathbb{O}$. De igual forma ocurre con G_2:

$$(G_2(w))^4 = \left(\sum_{n=-\infty}^{\infty} q^{n^2}\right)^4 = \sum_{n_1,n_2,n_3,n_4\in\mathbb{Z}} q^{n_1^2+n_2^2+n_3^2+n_4^2} = \sum_{k=0}^{\infty} q^k \sum_{n_1^2+n_2^2+n_3^2+n_4^2=k} 1 = \sum_{k=0}^{\infty} r_4^{\mathbb{Z}}(k)q^k = 1 + \sum_{k=1}^{\infty} r_4^{\mathbb{Z}}(k)q^k.$$

Al establecer las identidades $F_i(w^4) = (G_i(w))^4$ se deduce:

$$\sum_{\substack{k=1\\ k\in\mathbb{O}}}^{\infty} r_4^{\mathbb{O}}(4k)q^k = \sum_{\substack{k=1\\ k\in\mathbb{O}}}^{\infty} 16\sigma(k)q^k, \qquad \sum_{k=1}^{\infty} r_4^{\mathbb{Z}}(k)q^k = \sum_{k=1}^{\infty} 16\sigma_{\mathbb{O}}(k)q^{2k} + 8\sum_{k=1}^{\infty}\sigma_{\mathbb{O}}q^k = \sum_{k=1}^{\infty} f(k)q^k,$$

donde $f(k) = 8\sigma_{\mathbb{O}}(k) = 8\sigma(k)$ se k es impar y $f(k) = 16\sigma_{\mathbb{O}}(k/2) + 8\sigma_{\mathbb{O}}(k) = 24\sigma_{\mathbb{O}}(k)$ si k es par. Al restar ambas series en cada caso, se obtiene una serie de potencias nula en $q = e^{\pi i\tau}$ con $\mathrm{Im}(\tau) > 0$, por lo que los coeficientes de la serie de potencias deben ser cero, y así $r_4^{\mathbb{O}}(4k) = 16\sigma(k)$ y $r_4^{\mathbb{Z}}(k) = f(k)$, concluyendo las dos partes del enunciado.□

Gracias al *Teorema de los cuatro cuadrados de Jacobi*, es posible obtener la media de las funciones $r_4^{\mathbb{A}}(k)$ de la siguiente forma:

Proposicion 1.14 *Se tienen:*

$$\sum_{k\leq x} r_4^{\mathbb{Z}}(k) = \frac{\pi^2}{2}x^2 + \mathcal{O}(x\log x), \qquad \sum_{k\leq x} r_4^{\mathbb{O}}(k) = \frac{\pi^2}{12}x^2 + \mathcal{O}(x\log x).$$

Demostración. Para el caso $r_4^{\mathbb{Z}}(k)$, es posible agrupar la casuística dada por el *Teorema de los cuatro cuadrados de Jacobi* (Teorema 1.13) de manera que:

$$r_4^{\mathbb{Z}}(k) = 8\left(2+(-1)^k\right)\sigma_{\mathbb{O}}(k).$$

Sustituyendo $k = dn$ y aplicando (21):

$$\sum_{k\leq x} r_4^{\mathbb{Z}}(k) = 8\sum_{n\leq x}(2+(-1)^n)\sum_{\substack{dn\leq x\\ d \text{ impar}}} d = 8\sum_{n\leq x}(2+(-1)^n)\left(\sum_{d\leq \frac{x}{n}} d - 2\sum_{d\leq \frac{x}{2n}} d\right)$$

$$= 8\sum_{n\leq x}(2+(-1)^n)\left(\frac{x^2}{4n^2}+\mathcal{O}\left(\frac{x}{n}\right)\right) = 4\zeta(2)x^2 + 2x^2\sum_{n=1}^{\infty}\frac{(-1)^n}{n^2} - 2x^2\sum_{n>x}\frac{2+(-1)^n}{n^2} + \mathcal{O}\left(x\log x\right).$$

La primera suma puede expresarse en función de $\zeta(s)$ y la segunda se acota directamente por la integral:

$$\sum_{n=1}^{\infty}\frac{(-1)^n}{n^s} = \sum_{n=1}^{\infty}\frac{1}{(2n)^s} - \sum_{n=1}^{\infty}\frac{1}{(2n-1)^s} = 2\sum_{n=1}^{\infty}\frac{1}{(2n)^s} - \sum_{n=1}^{\infty}\frac{1}{n^s} = (2^{1-s}-1)\zeta(s).$$

$$\left|-2x^2\sum_{n>x}\frac{2+(-1)^n}{n^2}\right| \ll x^2\int_x^{\infty}\frac{dt}{t^2} = x.$$

Agrupando los resultados obtenidos se concluye:

$$\sum_{k\leq x} r_4^{\mathbb{Z}}(k) = 3\zeta(2)x^2 + \mathcal{O}(x) + \mathcal{O}(x\log x) = \frac{\pi^2}{2}x^2 + \mathcal{O}(x\log x).$$

Por otra parte, para el caso $r_4^{\mathbb{O}}(k)$ se procede de forma completamente análoga, obteniendo:

$$\sum_{k\leq x} r_4^{\mathbb{O}}(k) = \sum_{4n\leq x} r_4^{\mathbb{O}}(4n) = \sum_{n\leq \frac{x}{4}} 16\sigma(n) = 16\sum_{n\leq \frac{x}{4}}\sum_{d|n} d = 16\sum_{n\leq \frac{x}{4}}\sum_{d\leq \frac{x}{4n}} d = 8\sum_{n\leq \frac{x}{4}} \lfloor\frac{x}{4n}\rfloor\left(\lfloor\frac{x}{4n}\rfloor+1\right)$$

$$= \frac{x^2}{2}\sum_{n\leq \frac{x}{4}}\frac{1}{n^2} + \mathcal{O}\left(x\sum_{n\leq \frac{x}{4}}\frac{1}{n}\right) = \frac{x^2}{2}\left(\zeta(2)+\mathcal{O}\left(\frac{1}{x}\right)\right) + \mathcal{O}(x\log x) = \frac{\pi^2}{12}x^2 + \mathcal{O}(x\log x).$$

□

Con este resultado se podría deducir la *Ley de Weyl* para los grupos $\mathbf{SO}(8)$ y $\mathbf{SO}(9)$, pero la intención es emplearlo para construir los resultados análogos en los casos superiores (para $n > 4$). Para probar el paso del caso $n = 4$ a los casos superiores se necesitarán tres resultados de [**?**]. Para comenzar, se establece una relación sencilla entre los casos $n-1$ y n:

Lema 1.15 *Se tiene:*

$$\sum_{k\leq x} r_n^{\mathbb{A}}(k) = \sum_{\substack{|l|\leq\sqrt{x}\\ l\in\mathbb{A}}}\sum_{k\leq x-l^2} r_{n-1}^{\mathbb{A}}(k).$$

Demostración. Se deduce directamente:

$$\sum_{k\leq x} r_n^{\mathbb{A}}(k) = \sum_{k\leq x}\sum_{\substack{l^2\leq k\\ l\in\mathbb{A}}} r_{n-1}^{\mathbb{A}}(k-l^2) = \sum_{\substack{|l|\leq\sqrt{x}\\ l\in\mathbb{A}}}\sum_{k\leq x-l^2} r_{n-1}^{\mathbb{A}}(k).$$

□

A continuación se expresa una fórmula de recurrencia acerca del volumen de las bolas n-dimensionales:

Lema 1.16 *Si $\omega_n(t) = |\mathbb{B}_t^n|$ se verifica:*

$$\sum_{\substack{|l|\le\sqrt{x}\\ l\in\mathbb{Z}}} \omega_n(\sqrt{x-l^2}) = \omega_{n+1}(\sqrt{x}) + \mathcal{O}\left(x^{\frac{n-1}{2}}\right), \qquad \sum_{\substack{|l|\le\sqrt{x}\\ l\in\mathbb{O}}} \omega_n(\sqrt{x-l^2}) = \frac{1}{2}\omega_{n+1}(\sqrt{x}) + \mathcal{O}\left(x^{\frac{n-1}{2}}\right).$$

Demostración. Se tiene por definición:

$$\omega_{n+1}(\sqrt{t}) = \int\cdots\int_{\{u_1^2+\ldots+u_{n+1}^2\le t\}} du_1\cdots du_{n+1}$$
$$= \int_{\{|u|\le\sqrt{t}\}} \int\cdots\int_{\{u_1^2+\ldots+u_n^2\le t-u^2\}} du_1\cdots du_n du = \int_{-\sqrt{t}}^{\sqrt{t}} \omega_n(\sqrt{t-u^2})\,du.$$

Aplicando (16):

$$\sum_{\substack{|l|\le\sqrt{x}\\ l\in\mathbb{Z}}} \omega_n(\sqrt{x-l^2}) = \omega_n(\sqrt{x}) + 2\sum_{0<l\le\sqrt{x}} \omega_n(\sqrt{x-l^2})$$
$$= \omega_n(\sqrt{x}) + 2\left(\psi(0)\omega_n(\sqrt{x}) - \psi(\sqrt{x})\omega_n(0)\right) + 2\int_0^{\sqrt{x}} \omega_n(\sqrt{x-u^2})\,du + 2\int_0^{\sqrt{x}} \psi(u)\omega_n'(\sqrt{x-u^2})\,du$$
$$= \omega_{n+1}(\sqrt{x}) + \int_{-\sqrt{x}}^{\sqrt{x}} \psi(u)\omega_n'(\sqrt{x-u^2})\,du.$$

Basta ver que la integral que queda es $\mathcal{O}(x^{(n-1)/2})$. Para ello se recurre a la fórmula explícita de $\omega_n(t)$ dada por el Lema 1.2:

$$\omega_n'(\sqrt{x-u^2}) = \frac{d}{du}\left(\frac{\pi^{\frac{n}{2}}}{\Gamma\left(\frac{n}{2}+1\right)}\cdot(x-u^2)^{\frac{n}{2}}\right) = -n\omega_n(1)u(x-u^2)^{\frac{n}{2}-1}.$$

Por tanto:

$$\int_{-\sqrt{x}}^{\sqrt{x}} \psi(u)\omega_n'(\sqrt{x-u^2})\,du = -2n\omega_n(1)\int_0^{\sqrt{x}} \psi(u)u(x-u^2)^{\frac{n}{2}-1}\,du.$$

En el intervalo $[0,\sqrt{x}]$, la función $f(u)=u$ es positiva y creciente mientras que la función $f(u)=(x-u^2)^{n/2-1}$ es positiva y decreciente para $n>2$, por lo que es posible emplear el *Segundo Teorema del Valor Medio* para deducir que existen $\xi,\eta\in(0,\sqrt{x})$ tales que:

$$\int_0^{\sqrt{x}} \psi(u)u(x-u^2)^{\frac{n}{2}-1}\,du = \sqrt{x}\int_\xi^{\sqrt{x}} \psi(u)(x-u^2)^{\frac{n}{2}-1}\,du = \sqrt{x}(x-\xi^2)^{\frac{n}{2}-1}\int_\xi^\eta \psi(u)\,du$$

La integral de la función $\psi(u)$ es $\mathcal{O}(1)$ ya que en cada intervalo de extremos enteros $[n,n+1]$ es cero, por lo que:

$$\int_{-\sqrt{x}}^{\sqrt{x}} \psi(u)\omega_n'(\sqrt{x-u^2})\,du = -2n\omega_n(1)\sqrt{x}(x-\xi^2)^{\frac{n}{2}-1}\mathcal{O}(1) = \mathcal{O}\left(x^{\frac{n-1}{2}}\right).$$

Con esto se concluye la identidad para el caso $\mathbb{Z}$. Para probar el caso $\mathbb{O}$ se recurre al anterior de la siguiente forma:

$$\sum_{\substack{|l|\le\sqrt{x}\\ l\in\mathbb{O}}} \omega_n(\sqrt{x-l^2}) = \sum_{\substack{|l|\le\sqrt{x}\\ l\in\mathbb{Z}}} \omega_n(\sqrt{x-l^2}) - \sum_{\substack{|l|\le\sqrt{x}\\ l\in\mathbb{E}}} \omega_n(\sqrt{x-l^2}) = \omega_{n+1}(\sqrt{x}) + \mathcal{O}\left(x^{\frac{n-1}{2}}\right) - \sum_{|2l|\le\sqrt{x}} \omega_n(\sqrt{x-4l^2}).$$

La suma que aparece restando puede tratarse análogamente al caso $\mathbb{Z}$. Aplicando de nuevo (16) y tomando $v := 2u$:

$$\sum_{|2l|\le\sqrt{x}} \omega_n(\sqrt{x-4l^2}) = \omega_n(\sqrt{x}) + 2\sum_{0<l\le\frac{\sqrt{x}}{2}} \omega_n(\sqrt{x-4l^2})$$
$$= \omega_n(\sqrt{x}) + 2\left(\psi(0)\omega_n(\sqrt{x}) - \psi\left(\frac{\sqrt{x}}{2}\right)\omega_n(0)\right) + 2\int_0^{\frac{\sqrt{x}}{2}} \omega_n(\sqrt{x-4u^2})\,du + 2\int_0^{\frac{\sqrt{x}}{2}} \psi(u)\omega_n'(\sqrt{x-4u^2})\,du$$
$$= \frac{1}{2}\omega_{n+1}(\sqrt{x}) + \frac{1}{2}\int_{-\sqrt{x}}^{\sqrt{x}} \psi\left(\frac{v}{2}\right)\omega_n'(\sqrt{x-v^2})\,dv.$$

La integral que queda en este caso es esencialmente la misma que en el caso $\mathbb{Z}$ salvo constantes, por lo que también es $\mathcal{O}(x^{(n-1)/2})$. Incorporando esta estimación se concluye la identidad para el caso $\mathbb{O}$. □

El último resultado previo para pasar del caso $n = 4$ a los casos superiores consiste en expresar de forma especial la media de $r_4^{\mathbb{A}}(k)$, ligeramente distinta a las fórmulas calculadas en la Proposición 1.14:

Lema 1.17 *Se cumple:*

$$\sum_{k\leq x} r_4^{\mathbb{Z}}(k) = \omega_4(\sqrt{x}) + 8x\left(g\left(\frac{x}{4}\right) - g(x)\right) + \mathcal{O}(x), \qquad \sum_{k\leq x} r_4^{\mathbb{O}}(k) = \frac{1}{6}\omega_4(\sqrt{x}) - 4xg\left(\frac{x}{4}\right) + \mathcal{O}(x);$$

donde:

$$g(t) = \sum_{k\leq t} \frac{1}{k}\psi\left(\frac{t}{k}\right).$$

Demostración. Empezando por el caso $\mathbb{Z}$, gracias al *Teorema de los cuatro cuadrados de Jacobi* (Teorema 1.13) se tiene:

$$\sum_{k\leq x} r_4^{\mathbb{Z}}(k) = 1 + \sum_{\substack{k\leq x\\ k\in\mathbb{O}}} r_4^{\mathbb{Z}}(k) + \sum_{\substack{k\leq x\\ k\in\mathbb{E}}} r_4^{\mathbb{Z}}(k) = 1 + 8\sum_{\substack{k\leq x\\ k\in\mathbb{O}}} \sigma(k) + 24\sum_{k\leq \frac{x}{2}} \sigma_{\mathbb{O}}(k).$$

Sabiendo que:

$$\sum_{n\leq x}\sum_{2d|n} f(d) = \sum_{n\leq \frac{x}{2}}\sum_{d|n} f(d),$$

a través de esta identidad es posible estudiar cada una de las sumas anteriores por separado tomando como función auxiliar:

$$h(t) := \sum_{k\leq t} \sigma(k).$$

El resultado para cada suma es:

$$\sum_{k\leq \frac{x}{2}} \sigma_{\mathbb{O}}(k) = \sum_{k\leq \frac{x}{2}} \left(\sum_{d|k} d - \sum_{2d|k} 2d\right) = \sum_{k\leq \frac{x}{2}} \sigma(k) - 2\sum_{k\leq \frac{x}{2}}\sum_{2d|k} d = h\left(\frac{x}{2}\right) - 2\sum_{k\leq \frac{x}{4}} \sigma(k) = h\left(\frac{x}{2}\right) - 2h\left(\frac{x}{4}\right),$$

$$\sum_{\substack{k\leq x\\ k\in\mathbb{O}}} \sigma(k) = \sum_{k\leq x} \sigma(k) - \sum_{2j\leq x} \sigma(2j) = h(x) - \sum_{j\leq \frac{x}{2}} \left(\sum_{2d|2j} 2d + \sum_{\substack{d|2j\\ d\in\mathbb{O}}} d\right)$$
$$= h(x) - 2\sum_{j\leq \frac{x}{2}} \sigma(j) - \sum_{j\leq \frac{x}{2}} \sigma_{\mathbb{O}}(j) = h(x) - 3h\left(\frac{x}{2}\right) + 2h\left(\frac{x}{4}\right).$$

Sustituyendo estos cálculos se llega a:

$$\sum_{k\leq x} r_4^{\mathbb{Z}}(k) = 1 + 8h(x) - 32h\left(\frac{x}{4}\right).$$

El siguiente paso es encontrar una relación entre g y h. Más concretamente:

$$h(t) = \frac{\pi^2}{12}t^2 - tg(t) + \mathcal{O}(t).$$

En efecto, por (23):

$$h(t) = \sum_{k\leq t}\sum_{d|k} d = \sum_{j\leq t}\sum_{d\leq \frac{t}{j}} d = \frac{1}{2}\sum_{j\leq t}\left[\left(\frac{t}{j} - \psi\left(\frac{t}{j}\right)\right)^2 - \frac{1}{4}\right] = \frac{t^2}{2}\sum_{j\leq t}\frac{1}{j^2} - t\sum_{j\leq t}\frac{1}{j}\psi\left(\frac{t}{j}\right) + \frac{1}{2}\sum_{j\leq t}\left(\psi^2\left(\frac{t}{j}\right) - \frac{1}{4}\right)$$
$$= \frac{t^2}{2}\left(\frac{\pi^2}{6} + \mathcal{O}\left(\frac{1}{t}\right)\right) - tg(t) + \frac{1}{2}\sum_{j\leq t}\left(\left\{\frac{t}{j}\right\}^2 - \left\{\frac{t}{j}\right\}\right).$$

Puesto que se cumplen las desigualdades $-1 < \{t/j\}^2 - \{t/j\} < 1$, la suma que queda es $\mathcal{O}(t)$, y sustituyendo se obtiene la relación esperada entre g y h. Usando dicha relación y el Lema 1.2, se puede concluir:

$$\sum_{k\leq x} r_4^{\mathbb{Z}}(k) = 1 + 8\left(\frac{\pi^2}{12}x^2 - xg(x) + \mathcal{O}(x)\right) - 32\left(\frac{\pi^2}{12}\left(\frac{x}{4}\right)^2 - \frac{x}{4}g\left(\frac{x}{4}\right) + \mathcal{O}(x)\right)$$
$$= \omega_4(\sqrt{x}) + 8x\left(g\left(\frac{x}{4}\right) - g(x)\right) + \mathcal{O}(x).$$

Con esta deducción se prueba el caso $\mathbb{Z}$. Para finalizar, el caso $\mathbb{O}$ se obtiene directamente aplicando de nuevo el *Teorema de los cuatro cuadrados de Jacobi* (Teorema 1.13), el caso $\mathbb{Z}$ y la relación entre g y h:

$$\sum_{k\leq x} r_4^{\mathbb{O}}(k) = \sum_{4k\leq x} r_4^{\mathbb{O}}(4k) = 16\sum_{k\leq \frac{x}{4}} \sigma(k) = 16h\left(\frac{x}{4}\right)$$
$$= 16\left(\frac{\pi^2}{12}\left(\frac{x}{4}\right)^2 - \frac{x}{4}g\left(\frac{x}{4}\right) + \mathcal{O}\left(\frac{x}{4}\right)\right) = \frac{1}{6}\omega_4(\sqrt{x}) - 4xg\left(\frac{x}{4}\right) + \mathcal{O}(x).$$

□

Esta nueva formulación del caso $n = 4$ supone el punto de partida para obtener una estimación más fina en los casos superiores. El objetivo concreto es intentar eliminar el factor $\log x$ que aparece en los desarrollos asintóticos de la Proposición 1.14, que es lo que se ha obtenido para $n = 4$. Para poder hacerlo, se comienza estudiando si es posible para el caso $n = 5$ y de ahí se extiende al resto por inducción:

Proposicion 1.18 *Se cumple para todo $n \geq 5$:*

$$\sum_{k\leq x} r_n^{\mathbb{Z}}(k) = \omega_n(\sqrt{x}) + \mathcal{O}\left(x^{\frac{n}{2}-1}\right), \qquad \sum_{k\leq x} r_n^{\mathbb{O}}(k) = \frac{1}{6\cdot 2^{n-4}}\omega_n(\sqrt{x}) + \mathcal{O}\left(x^{\frac{n}{2}-1}\right).$$

Demostración. Empezando como se ha dicho por el caso $n = 5$, se aplican los Lemas 1.15, 1.16 y 1.17 obteniendo en cada caso:

$$\sum_{k\leq x} r_5^{\mathbb{Z}}(k) = \sum_{\substack{|l|\leq\sqrt{x}\\ l\in\mathbb{Z}}} \sum_{k\leq x-l^2} r_4^{\mathbb{Z}}(k) = \sum_{\substack{|l|\leq\sqrt{x}\\ l\in\mathbb{Z}}} \left(\omega_4(\sqrt{x-l^2}) - 8(x-l^2)\left(g(x-l^2) - g\left(\frac{x-l^2}{4}\right)\right) + \mathcal{O}(x-l^2)\right)$$
$$= \omega_5(\sqrt{x}) + \mathcal{O}\left(x^{\frac{3}{2}}\right) - 8\left(S_1(x) - S_2(x)\right) + \sum_{|l|\leq\sqrt{x}} \mathcal{O}(x-l^2),$$

$$\sum_{k\leq x} r_5^{\mathbb{O}}(k) = \sum_{\substack{|l|\leq\sqrt{x}\\ l\in\mathbb{O}}} \sum_{k\leq x-l^2} r_4^{\mathbb{O}}(k) = \sum_{\substack{|l|\leq\sqrt{x}\\ l\in\mathbb{O}}} \left(\frac{1}{6}\omega_4(\sqrt{x-l^2}) - 4(x-l^2)g\left(\frac{x-l^2}{4}\right) + \mathcal{O}(x-l^2)\right)$$
$$= \frac{1}{12}\omega_5(\sqrt{x}) + \mathcal{O}\left(x^{\frac{3}{2}}\right) + \mathcal{O}(S_2(x)) + \mathcal{O}\left(\sum_{|l|\leq\sqrt{x}} \mathcal{O}(x-l^2)\right);$$

donde:

$$S_1(x) = \sum_{|l|\leq\sqrt{x}} (x-l^2)g(x-l^2), \qquad S_2(x) = \sum_{|l|\leq\sqrt{x}} (x-l^2)g\left(\frac{x-l^2}{4}\right).$$

Por una parte, la suma de los términos de error verifica por (19):

$$\sum_{|l|\leq\sqrt{x}} \mathcal{O}(x-l^2) = \mathcal{O}\left(x\cdot\left(2\lfloor\sqrt{x}\rfloor + 1\right)\right) = \mathcal{O}\left(x^{\frac{3}{2}}\right).$$

Por otra parte, antes de estudiar las sumas $S_1(x)$ y $S_2(x)$ se consideran las sumas auxiliares:

$$A_1(l,x) = \sum_{j=1}^{l} g(x-j^2) = \sum_{m=1}^{x-1} \frac{1}{m} \sum_{j=1}^{\min\{l,\sqrt{x-m}\}} \psi\left(\frac{x-j^2}{m}\right),$$

$$A_2(l,x)=\sum_{j=1}^{l} g\left(\frac{x-j^2}{4}\right)=\sum_{m=1}^{x-1}\frac{1}{m}\sum_{j=1}^{\min\{l,\sqrt{x-4m}\}}\psi\left(\frac{x-j^2}{4m}\right).$$

Tomando $f(l)=(x-l^2)/m$, $a=1$ y $b=\min\{l,\sqrt{x-m}\}$ en la suma interior de $A_1(x)$ y $f(l)=(x-l^2)/(4m)$, $a=1$ y $b=\min\{l,\sqrt{x-4m}\}$ en la suma interior de $A_2(x)$ es posible aplicar la siguiente estimación de van der Corput [**?**]:

$$\sum_{a\le j\le b}\psi(f(j))\ll |f'(b)-f'(a)|\lambda^{-\frac{2}{3}}+\lambda^{-\frac{1}{2}},\qquad 0<\lambda\le 1,\quad f''(x)\ge\lambda \text{ o } f''(x)\le-\lambda \text{ para todo } x\in[a,b].$$

De aquí se deduce para todo $l\le\sqrt{x}$:

$$A_1(l,x)\ll\sum_{m=1}^{x-1}\frac{1}{m}\left(\left|\frac{2a}{m}-\frac{2b}{m}\right|\cdot\left(\frac{2}{m}\right)^{-\frac{2}{3}}+\left(\frac{2}{m}\right)^{-\frac{1}{2}}\right)$$
$$\ll\sum_{m=1}^{x-1}\frac{1}{m}\left(m^{-\frac{1}{3}}\sqrt{x}+\sqrt{m}\right)\le\zeta\left(\frac{4}{3}\right)\sqrt{x}+\sum_{m=1}^{x}m^{-\frac{1}{2}}\ll\sqrt{x}.$$

$$A_2(l,x)\ll\sum_{m=1}^{x-1}\frac{1}{m}\left(\left|\frac{a}{2m}-\frac{b}{2m}\right|\cdot\left(\frac{1}{2m}\right)^{-\frac{2}{3}}+\left(\frac{1}{2m}\right)^{-\frac{1}{2}}\right)\ll\sum_{m=1}^{x-1}\frac{1}{m}\left(m^{-\frac{1}{3}}\sqrt{x}+\sqrt{m}\right)\ll\sqrt{x}.$$

Teniendo en cuenta que por (21) se cumple directamente que $g(t)=\mathcal{O}(\log t)$, se puede proceder a estimar $S_1(x)$ y $S_2(x)$ utilizando (13):

$$S_1(x)=2\sum_{l\le\sqrt{x}}(x-l^2)g(x-l^2)+xg(x)$$
$$=2\sum_{l=1}^{\lfloor\sqrt{x}\rfloor-1}\left((x-l^2)-(x-(l+1)^2)\right)A_1(l,x)+2\left(x-\lfloor\sqrt{x}\rfloor^2\right)A_1(\lfloor\sqrt{x}\rfloor,x)+\mathcal{O}(x\log x)$$
$$=2\sum_{l=1}^{\lfloor\sqrt{x}\rfloor-1}(2l+1)\mathcal{O}(\sqrt{x})+\mathcal{O}\left(x^{\frac{3}{2}}\right)+\mathcal{O}(x\log x)=\mathcal{O}\left(x^{\frac{3}{2}}\right),$$

$$S_2(x)=2\sum_{l\le\sqrt{x}}(x-l^2)g\left(\frac{x-l^2}{4}\right)+xg\left(\frac{x}{4}\right)$$
$$=2\sum_{l=1}^{\lfloor\sqrt{x}\rfloor-1}\left((x-l^2)-(x-(l+1)^2)\right)A_2(l,x)+2\left(x-\lfloor\sqrt{x}\rfloor^2\right)A_2(\lfloor\sqrt{x}\rfloor,x)+\mathcal{O}(x\log x)$$
$$=2\sum_{l=1}^{\lfloor\sqrt{x}\rfloor-1}(2l+1)\mathcal{O}(\sqrt{x})+\mathcal{O}\left(x^{\frac{3}{2}}\right)+\mathcal{O}(x\log x)=\mathcal{O}\left(x^{\frac{3}{2}}\right).$$

Sustituyendo todas las estimaciones obtenidas y agrupando los términos de error se concluye:

$$\sum_{\substack{k\le x\\ k\in\mathbb{Z}}}r_5^{\mathbb{Z}}(k)=\omega_5(\sqrt{x})+\mathcal{O}\left(x^{\frac{3}{2}}\right),\qquad\sum_{\substack{k\le x\\ k\in\mathbb{O}}}r_5^{\mathbb{Z}}(k)=\frac{1}{12}\omega_5(\sqrt{x})+\mathcal{O}\left(x^{\frac{3}{2}}\right).$$

Una vez establecido el caso $n=5$ basta suponer ciertas las identidades del enunciado hasta $n-1$ y utilizar inducción para n recurriendo de nuevo a los Lemas 1.15 y 1.16 y a (19). El resultado es:

$$\sum_{k\le x}r_n^{\mathbb{Z}}(k)=\sum_{\substack{|l|\le\sqrt{x}\\ l\in\mathbb{Z}}}\sum_{k\le x-l^2}r_{n-1}^{\mathbb{Z}}(k)=\sum_{\substack{|l|\le\sqrt{x}\\ l\in\mathbb{Z}}}\left(\omega_{n-1}(\sqrt{x-l^2})+\mathcal{O}\left((x-l^2)^{\frac{n-3}{2}}\right)\right)$$
$$=\omega_n(\sqrt{x})+\mathcal{O}\left(x^{\frac{n}{2}-1}\right)+\sum_{|l|\le\sqrt{x}}\mathcal{O}\left((x-l^2)^{\frac{n-3}{2}}\right)=\omega_n(\sqrt{x})+\mathcal{O}\left(x^{\frac{n}{2}-1}\right),$$

$$\sum_{k\le x} r_n^{\mathbb{O}}(k) = \sum_{\substack{|l|\le\sqrt{x}\\ l\in\mathbb{O}}} \sum_{k\le x-l^2} r_{n-1}^{\mathbb{O}}(k) = \sum_{\substack{|l|\le\sqrt{x}\\ l\in\mathbb{O}}} \left(\frac{1}{6\cdot 2^{n-5}}\omega_{n-1}(\sqrt{x-l^2}) + \mathcal{O}\left((x-l^2)^{\frac{n-3}{2}}\right)\right)$$

$$= \frac{1}{6\cdot 2^{n-4}}\omega_n(\sqrt{x}) + \mathcal{O}\left(x^{\frac{n}{2}-1}\right) + \mathcal{O}\left(\sum_{|l|\le\sqrt{x}} \mathcal{O}\left((x-l^2)^{\frac{n-3}{2}}\right)\right) = \frac{1}{6\cdot 2^{n-4}}\omega_n(\sqrt{x}) + \mathcal{O}\left(x^{\frac{n}{2}-1}\right).$$

□

D. Paso 4 - Conclusión. Con todos los requisitos anteriores es posible probar el resultado principal:

Teorema 1.19 (Chamizo-G.) *Para todo $n \ge 4$ se cumple:*

$$\mathcal{N}(\lambda) = C_d\lambda^{\frac{d}{2}} + \mathcal{O}\left(\lambda^{\frac{d}{2}-1}\Phi_n(\lambda)\right), \qquad \Phi_n(\lambda) = \begin{cases}\log\lambda & si\ n=4,\\ 1 & si\ n>4.\end{cases}$$

donde $d = \dim(\mathbf{SO}(N))$ y C_d es la constante que proporciona la Ley de Weyl.

Demostración. Si se reagrupan los desarrollos asintóticos estudiados en el apartado anterior para $x = R_N^2$, se verifican las fórmulas:

$$\sum_{k\le R_N^2} r_n^{\mathbb{A}}(k) = C_{2,N}\omega_n(R_N) + \mathcal{O}\left(R_N^{n-2}\Phi_n(R_N)\right), \qquad C_{2,N} := \begin{cases}1 & \text{si } N=2n,\\ \frac{1}{6\cdot 2^{n-4}} & \text{si } N=2n+1.\end{cases}$$

Utilizando ahora (14) para $a_k = r_n^{\mathbb{A}}(k)$ y $f(k) = k^{(d-n)/2}$, la suma del término principal de $\mathcal{N}(\lambda)$ se traduce en lo siguiente:

$$\sum_{k\le R_N^2} k^{\frac{d-n}{2}} r_n^{\mathbb{A}}(k)$$

$$= \left(C_{2,N}\omega_n(R_n) + \mathcal{O}\left(R_N^{n-1}\Phi_n(R_N)\right)\right)R_N^{d-n} + \mathcal{O}(1) - \frac{d-n}{2}\int_1^{R_N^2}\left(C_{2,N}\omega_n(t) + \mathcal{O}\left(t^{\frac{n}{2}-1}\Phi_n(t)\right)\right)t^{\frac{d-n}{2}-1}\,dt$$

$$= \frac{n}{d}C_{2,N}R_N^d + \mathcal{O}\left(R_N^{d-2}\Phi_n(R_N)\right).$$

Con esta deducción es posible expresar $\mathcal{N}(\lambda)$ tomando $C_N := C_{1,N}\cdot C_{2,N}$ agrupando los términos de error en términos de R_N de la siguiente forma:

$$\mathcal{N}(\lambda) = \frac{n}{d}P_0C_N\omega_n(1)R_N^d + \mathcal{O}\left(R_N^{d-2}\Phi_n(R_N)\right).$$

Si se toma $\kappa_N := 1$ si $N = 2n$ y $\kappa_N := 2$ si $N = 2n+1$, entonces $R_N = \kappa_N\lambda^{1/2}(1+\mathcal{O}(\lambda^{-1}))$. Sustituyendo y empleando el desarrollo de Taylor $(1+t)^\alpha = 1+\mathcal{O}(t)$ para todo $\alpha > 0$ y $|t| < 1$, se concluye:

$$\mathcal{N}(\lambda) = \frac{n}{d}P_0C_N\omega_n(1)\kappa_N^d\lambda^{\frac{d}{2}}(1+\mathcal{O}(\lambda^{-1})) + \mathcal{O}\left(\lambda^{\frac{d}{2}-1}(1+\mathcal{O}(\lambda^{-1}))\Phi_n\left(\kappa_N\lambda^{\frac{1}{2}}(1+\mathcal{O}(\lambda^{-1}))\right)\right)$$

$$= \frac{n}{d}P_0C_N\omega_n(1)\kappa_N^d\lambda^{\frac{d}{2}} + \mathcal{O}\left(\lambda^{\frac{d}{2}-1}\Phi_n(\lambda)\right).$$

Puesto que la *Ley de Weyl* se debe satisfacer, la constante del término principal de $\mathcal{N}(\lambda)$ es para todo $n \ge 4$:

$$C_d := \frac{n}{d}P_0C_N\omega_n(1)\kappa_N^d = \frac{\mathrm{Vol}(\mathbf{SO}(N))}{(4\pi)^{\frac{d}{2}}\Gamma\left(\frac{d}{2}+1\right)}.$$

Con esto se concluye la prueba. □

E. Precisión del término de error. Una de las cuestiones que surgen tras este análisis de la Ley de Weyl es si realmente el término de error que se obtiene tras emplear los métodos descritos anteriormente es óptimo o bien puede reducirse en algún orden de magnitud. Observando el resultado general enunciado en [**?**], parece sugerir que en efecto dicho término es óptimo. Sin embargo, es posible sacar provecho de la interpretación aritmética con la que se ha realizado el análisis para comprobar la precisión del término de error sin apelar a este resultado general. Para poder llegar a ello, se parte de lo siguiente:

Lema 1.20 *Para todo k y para $n > 4$ se cumple que $r_n^{\mathbb{A}}(k) > C_n k^{\frac{n}{2}-1}$, siempre que $4 \mid k-n$ en el caso $\mathbb{A} = \mathbb{O}$.*

Demostración. Recuperando de nuevo el *Teorema de los cuatro cuadrados de Jacobi*(Teorema 1.13) se tiene:

$$r_4^{\mathbb{Z}}(k) = 8\left(2+(-1)^k\right)\sigma_{\mathbb{O}}(k); \qquad r_4^{\mathbb{O}}(k) = 16\sigma\left(k/4\right) \quad (\text{si } 4|k).$$

Si $n > 4$ puede escribirse $k = x_1^2+x_2^2+x_3^2+x_4^2+l$, donde $l := x_5^2+\ldots+x_n^2$. El número l será en general un número arbitrario, por lo que los sumandos que lo componen cumplirán que $0 \le |x_5|, \ldots, |x_n| \le \sqrt{l/(n-4)}$. En el caso en que los x_j sean enteros sin restricción, el caso en que menos representaciones de $k-l$ existen como suma de cuatro cuadrados es el caso en que $k-l$ sea impar y se tendría $r_4^{\mathbb{Z}}(k-l) \ge 8(k-l)$. Puesto que k no tiene condiciones de congruencia, siempre se puede acotar inferiormente dependiendo de los x_j extrayendo un subconjunto de los mismos que garantice que $k-l$ sea impar. Así se deduce:

$$\begin{aligned} r_n^{\mathbb{Z}}(k) = \sum_{l\le k} r_4^{\mathbb{Z}}(k-l) &\ge \sum_{\substack{x_5,\ldots,x_n \le \sqrt{k/(2n-8)} \\ 2\nmid k-x_5,\, 2|x_6,\ldots,x_n}} r_4^{\mathbb{Z}}\left(k-x_5^2-\ldots-x_n^2\right) \ge \sum_{\substack{x_5,\ldots,x_n \le \sqrt{k/(2n-8)} \\ 2\nmid k-x_5,\, 2|x_6,\ldots,x_n}} 8\left(k-x_5^2-\ldots-x_n^2\right) \\ &\ge 8 \sum_{\substack{x_5,\ldots,x_n \le \sqrt{k/(2n-8)} \\ 2\nmid k-x_5,\, 2|x_6,\ldots,x_n}} \left(k-(n-4)\cdot\frac{k}{2(n-4)}\right) \ge k \sum_{\substack{x_5,\ldots,x_n \le \sqrt{k/(2n-8)} \\ 2\nmid k-x_5,\, 2|x_6,\ldots,x_n}} 1 \gg_n k\cdot k^{\frac{n-4}{2}} = k^{\frac{n}{2}-1}. \end{aligned}$$

Por otra parte, si x_j es impar, entonces $x_j^2 \equiv 1 \pmod 4$ y así $k = x_1^2+\ldots+x_n^2 \equiv n \pmod 4$. Esto quiere decir que solo se tienen representaciones de $k-l$ si $4|k-l$, y en ese caso, $r_4^{\mathbb{O}}(k-l) = 16\sigma((k-l)/4) \ge 4(k-l)$. Teniendo en cuenta esta condición de congruencia se tendría de forma similar al caso anterior:

$$\begin{aligned} r_n^{\mathbb{O}}(k) = \sum_{\substack{l\le k \\ 4|k-l,\, x_i\in\mathbb{O}}} r_4^{\mathbb{O}}(k-l) &\ge \sum_{\substack{x_5,\ldots,x_n \le \sqrt{k/(2n-8)} \\ 4|k-n,\, x_i\in\mathbb{O}}} r_4^{\mathbb{O}}\left(k-x_5^2-\ldots-x_n^2\right) \\ &\ge \sum_{\substack{x_5,\ldots,x_n \le \sqrt{k/(2n-8)} \\ 4|k-n,\, x_i\in\mathbb{O}}} 4\left(k-x_5^2-\ldots-x_n^2\right) \ge 4 \sum_{\substack{x_5,\ldots,x_n \le \sqrt{k/(2n-8)} \\ 4|k-n,\, x_i\in\mathbb{O}}} \left(k-(n-4)\cdot\frac{k}{2(n-4)}\right) \\ &\ge k \sum_{\substack{x_5,\ldots,x_n \le \sqrt{k/(2n-8)} \\ 4|k-n,\, x_i\in\mathbb{O}}} 1 \gg_n k\cdot k^{\frac{n-4}{2}} = k^{\frac{n}{2}-1}. \end{aligned}$$

□

Volviendo atrás en la expresión para $\mathcal{N}(\lambda)$, únicamente habiendo sustituido los cálculos para los términos de error se obtendría en general tanto para $n = 4$ como para $n > 4$:

$$\mathcal{N}(\lambda) = C \sum_{k\le R_N^2} k^{\frac{d-n}{2}} r_n^{\mathbb{A}}(k) + \mathcal{O}\left(R_N^{d-\frac{n}{2}} \log R_N\right).$$

Con esta expresión se puede deducir lo siguiente:

Proposicion 1.21 *Sea la expresión de $\mathcal{N}(\lambda)$ en la forma anterior.*

(*A*) *Para $n > 4$ no es posible sustituir el término de error $\mathcal{O}(\lambda^{d/2-1})$ por $o(\lambda^{d/2-1})$ ni extraer un segundo término principal.*

(*B*) *Para $n = 4$ no es posible sustituir el término de error $\mathcal{O}(\lambda^{d/2-1}\log\lambda)$ por $o(\lambda^{d/2-1}\log\log\lambda)$.*

Demostración.

(*A*) Gracias al Lema 1.20, cada vez que R_N^2 alcanza un entero, la función $\mathcal{N}(\lambda)$ incrementa una cantidad comparable a $(R_N^2)^{(d-n)/2} r_n^{\mathbb{A}}(R_N^2) \asymp R_N^{d-n} R_N^{2\cdot(n/2-1)} = R_N^{d-2}$. Esto imposibilita sustituir el término de error $\mathcal{O}(\lambda^{d/2-1})$ por $o(\lambda^{d/2-1})$ o extraer un segundo término principal para $\mathcal{N}(\lambda)$.

(*B*) En el caso $N = 8$, sea $k = p_2 p_3 \cdots p_m$ el producto de los primeros primos impares. Por el *Teorema de los cuatro cuadrados de Jacobi* (Teorema 1.13) se tiene:

$$\frac{r_4^{\mathbb{Z}}(k)}{k} = \frac{8(2+(-1)^k)}{k} \sum_{\substack{d|k \\ d\in\mathbb{O}}} d = 8 \sum_{d|k} d^{-1} = 8 \left(\sum_{d|p_2} d^{-1} \right) \cdots \left(\sum_{d|p_m} d^{-1} \right)$$
$$= \frac{8 \prod_{j=2}^m (1+p_j^{-1}) \prod_{j=2}^m (1-p_j^{-1})}{\prod_{j=2}^m (1-p_j^{-1})} = \frac{8 \prod_{j=2}^m (1-p_j^{-2})}{\prod_{j=2}^m (1-p_j^{-1})} \sim \frac{8/\zeta(2)}{e^{-\gamma}/\log p_m} = \frac{48e^\gamma}{\pi^2} \log p_m.$$

El *Teorema de los Números Primos* sostiene que para $x \geq 2$:

$$\theta(x) := \sum_{p \leq x} \log p \sim x,$$

de donde $k = e^{\log k} = e^{\sum_{j=2}^m \log p_j} = e^{\theta(p_m) - \log 2} = e^{\theta(p_m)}/2 \sim e^{p_m}/2$. Al tomar logaritmos, $\log\log k \sim \log\log(e^{p_m}/2) = \log(p_m - \log 2) \sim \log p_m$, y así se deduce que $r_4^{\mathbb{Z}}(k) \sim 48e^\gamma/\pi^2 \cdot k \log\log k$. Para $k = R_N^2$ se tendría que $R_N^2 \log\log R_N \sim \lambda \log\log\lambda$ y cuando R_N^2 alcanza un entero, de nuevo gracias al Lema 1.20 la función $\mathcal{N}(\lambda)$ incrementa una cantidad comparable a $(R_N^2)^{d/2-2} r_4^{\mathbb{Z}}(R_N^2) \asymp R_N^{d-4} R_N^2 \log\log R_N^2 = R_N^{d-2} \log\log R_N^2$. Esto imposibilita sustituir el término de error $\mathcal{O}(\lambda^{d/2-1}\log\lambda)$ por $o(\lambda^{d/2-1}\log\log\lambda)$ en $\mathcal{N}(\lambda)$. El caso $N = 9$ se deduce igual tomando $k = 4p_2 p_3 \cdots p_m$, ya que en este caso el *Teorema de los cuatro cuadrados de Jacobi* (Teorema 1.13) implica:

$$\frac{r_4^{\mathbb{O}}(k)}{k} = \frac{16}{k} \sum_{d|k/4} d = 4 \sum_{d|k/4} d^{-1} \sim \frac{24e^\gamma}{\pi^2} \log p_m,$$

de donde $r_4^{\mathbb{O}}(k) \sim 24e^\gamma/\pi^2 \cdot k \log\log k$. Esto impide otra vez cambiar $\mathcal{O}(\lambda^{d/2-1}\log\lambda)$ por $o(\lambda^{d/2-1}\log\log\lambda)$ en $\mathcal{N}(\lambda)$. □

Para el caso $n = 4$, siguiendo técnicas de [**?**] es posible afinar un poco más la estimación del término de error $\mathcal{O}(R_N^{d-n/2}\log R_N)$ de $\mathcal{N}(\lambda)$ para conseguir $\mathcal{O}(R_N^{d-\alpha_0})$ para $\alpha_0 > 2$. Por otra parte, al estimar el término principal, es posible rebajar un factor $\log R_N$ a $(\log R_N)^{2/3}$ a través de métodos avanzados propios de Korobov y Vinogradov [**?**], lo cual produce al final el término $\mathcal{O}(\lambda^{d/2-1}(\log\lambda)^{2/3})$. Como se puede observar, hay un salto entre el factor $(\log\lambda)^{2/3}$ y el factor $\log\log\lambda$ que se ha obtenido anteriormente en ciertos casos, lo cual sigue siendo hoy en día un problema abierto [**?**].

§3. La Ley de Weyl en $\mathbf{SO}(N)$ para $N < 8$

Los casos contemplados en el Teorema 1.19 corresponden como se ha visto a $N \geq 8$ ($n \geq 4$), debido a que el procedimiento que se ha seguido durante todo el Capítulo excluye los seis casos inferiores $N = 2, 3, 4, 5, 6, 7$. Para ver un desarrollo asintótico que describa la *Ley de Weyl* en cada uno estos casos se utilizarán otros procedimientos, de forma que se pueden obtener los siguientes resultados:

Proposicion 1.22 (Chamizo-G.) *Para $n = 1$ existen constantes positivas C_1 y C_3 tales que:*

(*A*) *En* $\mathbf{SO}(2)$*:* $\mathcal{N}(\lambda) = C_1\lambda^{1/2} + \mathcal{O}(1)$.

(*B*) *En* $\mathbf{SO}(3)$*:* $\mathcal{N}(\lambda) = C_3\lambda^{3/2} + \mathcal{O}(\lambda)$.

Demostración.

(*A*) Se tiene la isometría $\mathbf{SO}(2) \cong S^1$, ya que $\mathbf{SO}(2)$ viene determinado por el ángulo de rotación. Por ello, la *Ley de Weyl* se puede establecer resolviendo el problema:

$$\begin{cases} -y'' = \lambda y \\ y(0) = y(2\pi) \quad (\lambda > 0) \end{cases}$$

La solución de la ecuación diferencial viene dada por $y(x) = e^{\pm i\sqrt{\lambda}x}$ e imponiendo la condición $y(0) = y(2\pi)$, entonces $1 = e^{\pm 2\pi i\sqrt{\lambda}}$, para lo cual, $\sqrt{\lambda} \in \mathbb{N}$. De esta forma, los autovalores son de la forma $\lambda = k^2$ con $k \in \mathbb{Z}$, cuya multiplicidad es 2, y las autofunciones corresponden a $\{e^{\pm ikx}\}_{k\in\mathbb{N}} = \{e^{ikx}\}_{k\in\mathbb{Z}}$. Por tanto:

$$\mathcal{N}(\lambda) = \sum_{l^2\leq\lambda} 1 = 2\lfloor\sqrt{\lambda}\rfloor + 1 = 2\lambda^{\frac{1}{2}} + \mathcal{O}(1).$$

El término de error es preciso, pues cada vez que λ alcanza un cuadrado, $\mathcal{N}(\lambda)$ aumenta en 1.

(B) En el caso $\mathbf{SO}(3)$ los autovalores son de la forma $l(l+1)$, correspondientes al operador momento angular en física cuántica, cuya multiplicidad es $(2l+1)^2$. Así, puesto que $\sum_{j=1}^{m}(2j-1)^2 = (2m-1)2m(2m+1)/6$, se deduce:

$$\mathcal{N}(\lambda) = \sum_{l(l+1)\leq\lambda}(2l+1)^2 = \sum_{l=0}^{\lfloor\sqrt{\lambda+\frac{1}{4}}-\frac{1}{2}\rfloor}(2l+1)^2 = \frac{4}{3}\left(\lambda+\frac{1}{4}\right)^{\frac{3}{2}} + \mathcal{O}(\lambda) = \frac{4}{3}\lambda^{\frac{3}{2}}\left(1+\frac{1}{4\lambda}\right)^{\frac{3}{2}} + \mathcal{O}(\lambda).$$

Si $1/(4\lambda) < 1$, el factor residual $(1+1/(4\lambda))^{3/2}$ es $1+\mathcal{O}(\lambda^{-1})$ por el desarrollo de Taylor, y si $0 < \lambda \leq 1/4$, entonces directamente $\sqrt{\lambda+1/4} - 1/2 = \mathcal{O}(1)$. En conclusión:

$$\mathcal{N}(\lambda) = \frac{4}{3}\lambda^{\frac{3}{2}} + \mathcal{O}(\lambda).$$

De nuevo, el término de error es preciso, ya que cuando λ alcanza un $l(l+1)$, $\mathcal{N}(\lambda)$ aumenta en algo comparable a $l^2 \sim \lambda$. □

Proposicion 1.23 (Chamizo-G.) *Para $n = 2$, existen constantes positivas C_6 y C_{10} tales que:*

(A) *En* $\mathbf{SO}(4)$*: $\mathcal{N}(\lambda) = C_6\lambda^3 + \mathcal{O}(\lambda^{2+27/82})$.*

(B) *En* $\mathbf{SO}(5)$*: $\mathcal{N}(\lambda) = C_{10}\lambda^5 + \mathcal{O}(\lambda^{4+27/82})$.*

Demostración.

(A) El polinomio que define la multiplicidad de los autovalores es $m_4(x,y) = (x^2-y^2)^2$. Por tanto, siendo $R_4^2 = \lambda + 1$ y suponiendo $y > x$, se tiene por las simetrías de $m_4(\vec{x})$:

$$\mathcal{N}(\lambda) = \frac{1}{4}\sum_{\vec{x}\in\mathbb{Z}^2} m_4(x,y)\chi_{R_4}(\vec{x}) = 2\sum_{0\leq x\leq\frac{R_4}{\sqrt{2}}}{}' \sum_{y\in I_x} m(x,y), \qquad I_x := \left(x, \sqrt{R_4^2-x^2}\right];$$

donde la prima $'$ indica que el término $x = 0$ aparece multiplicado por $1/2$. Aplicando (16) a la suma interior se obtiene:

$$\sum_{y\in I_x} m_4(x,y) = \psi\left(\sqrt{R_4^2-x^2}\right) m_4\left(x,\sqrt{R_4^2-x^2}\right) + \int_x^{\sqrt{R_4^2-x^2}} m_4(x,y)\,dy + \int_x^{\sqrt{R_4^2-x^2}} \frac{\partial m_4(x,y)}{\partial y}\psi(y)\,dy,$$

y sustituyendo en $\mathcal{N}(\lambda)$ se tiene la expresión $\mathcal{N}(\lambda) = \mathcal{N}_1 + \mathcal{N}_2 + \mathcal{N}_3$, donde:

$$\mathcal{N}_1 = 2\sum_{0\leq x\leq\frac{R_4}{\sqrt{2}}}{}' \int_x^{\sqrt{R_4^2-x^2}} m_4(x,y)\,dy, \qquad \mathcal{N}_2 = 2\sum_{0\leq x\leq\frac{R_4}{\sqrt{2}}}{}' \int_x^{\sqrt{R_4^2-x^2}} \frac{\partial m_4(x,y)}{\partial y}\psi(y)\,dy,$$

$$\mathcal{N}_3 = 2\sum_{0\leq x\leq\frac{R_4}{\sqrt{2}}}{}' \psi\left(\sqrt{R_4^2-x^2}\right) m_4\left(x,\sqrt{R_4^2-x^2}\right).$$

Para el término $\mathcal{N}_1$, se separa la contribución de $x = 0$ y se aplica de nuevo (16), consiguiendo:

$$\mathcal{N}_1 = 2\int_0^{\frac{R_4}{\sqrt{2}}}\int_x^{\sqrt{R_4^2-x^2}} m_4(x,y)\,dx\,dy - 2\int_0^{\frac{R_4}{\sqrt{2}}} \frac{x}{\sqrt{R_4^2-x^2}} m_4\left(x,\sqrt{R_4^2-x^2}\right)\psi(x)\,dx.$$

Aprovechando como en otras ocasiones que la integral de $\psi(x)$ es $\mathcal{O}(1)$ por el *Segundo Teorema del Valor Medio*, en dos puntos intermedios ξ y η, la segunda de las integrales de $\mathcal{N}_1$ puede acotarse así:

$$\left|\int_0^{\frac{R_4}{\sqrt{2}}} \frac{x}{\sqrt{R_4^2-x^2}} m_4\left(x,\sqrt{R_4^2-x^2}\right)\psi(x)\,dx\right| \ll \max_{[0,\frac{R_4}{\sqrt{2}}]} \frac{x(R_4^2-2x^2)^2}{\sqrt{R_4^2-x^2}} \cdot \left|\int_\xi^\eta \psi(x)\,dx\right| \ll R_4^4.$$

De esta forma, volviendo a tener en cuenta las simetrías de m_4 se satisface:

$$\mathcal{N}_1 = \frac{1}{4}\int_{\mathbb{R}^2} m_4(\vec{x})\chi_{R_4}(\vec{x})\,d\vec{x} + \mathcal{O}(R_4^4).$$

Por otra parte, para el término $\mathcal{N}_2$ se procede de forma similar:

$$\mathcal{N}_2 = 2\sum_{0\le x\le \frac{R_4}{\sqrt{2}}}{}' \int_x^{\sqrt{R_4^2-x^2}} 4y(y^2-x^2)\psi(y)\,dy \ll \sum_{0\le x\le \frac{R_4}{\sqrt{2}}}{}' R_4^3\left|\int_\xi^\eta \psi(y)\,dy\right| \ll R_4^4.$$

Por último, para el término $\mathcal{N}_3$ es posible aprovechar otro aspecto de la función $\psi(x)$. Más concretamente, la existencia de dos series de Fourier finitas [**?**] para cada M entero positivo:

$$Q^\pm(x) := \sum_{|m|\le M} a_m^\pm e^{2\pi i m x}$$

tales que $a_0^\pm = \mathcal{O}(M^{-1})$, $a_m^\pm = \mathcal{O}(m^{-1})$ y $Q^-(x) \le \psi(x) \le Q^+(x)$. Situando esta acotación en el término $\mathcal{N}_3$ se tiene:

$$2\sum_{|m|\le M} a_m^- S(m) \le \mathcal{N}_3 \le 2\sum_{|m|\le M} a_m^+ S(m),$$

donde:

$$\begin{aligned} S(m) &:= \sum_{0\le x\le \frac{R_4}{\sqrt{2}}}{}' m_4\left(x,\sqrt{R_4^2-x^2}\right) e^{2\pi i m\sqrt{R_4^2-x^2}} \\ &= \frac{1}{2}R_4^4 e^{2\pi i m R_4} + \sum_{1\le 2^\nu\le \frac{R_4}{\sqrt{2}}} \sum_{\frac{R_4}{\sqrt{2}\cdot 2^{\nu+1}}<x\le \frac{R_4}{\sqrt{2}\cdot 2^\nu}} \left(R_4^2-2x^2\right)^2 e^{2\pi i m\sqrt{R_4^2-x^2}} \end{aligned}$$

En la suma interior de S es posible aplicar (26) al término exponencial tomando $f(x) = m\sqrt{R_4^2-x^2}$, de forma que $|f'(x)| = |m|x/\sqrt{R_4^2-x^2} \le |m|/\sqrt{2^{2\nu+1}-1}$ en el intervalo $R_4/\sqrt{2}\cdot(2^{-\nu-1}, 2^{-\nu}]$ y escogiendo un par de exponentes (k,ℓ) se tiene:

$$\begin{aligned} |\mathcal{N}_3| &\ll \left(|a_0^+| + |a_0^-|\right) R_4^5 \\ &\quad + \sum_{1\le|m|\le M} \left(|a_m^+| + |a_m^-|\right) R_4^4 \left[1 + \sum_{1\le 2^\nu\le \frac{R_4}{\sqrt{2}}} \left(1-\frac{1}{2^{2\nu+2}}\right)^2 \left(\frac{|m|}{\sqrt{2^{2\nu+1}-1}}\right)^k \left(\frac{R_4}{2^{\nu+1}\sqrt{2}}\right)^\ell\right] \\ &\ll M^{-1}R_4^5 + R_4^{\ell+4} \sum_{1\le|m|\le M} |m|^{k-1} \sum_{1\le 2^\nu\le \frac{R_4}{\sqrt{2}}} \left(1-\frac{1}{2^{2\nu+2}}\right)^2 \left(\frac{1}{2\sqrt{2^{2\nu+1}-1}}\right)^k \left(\frac{1}{2^{\nu+1}\sqrt{2}}\right)^\ell \\ &\ll M^{-1}R_4^5 + M^k R_4^{\ell+4}. \end{aligned}$$

Al optimizar la estimación obtenida igualando los sumandos se tiene $M = R_4^{(1-\ell)/(1+k)}$. Así, usando el par $BA^3B(0,1) = (11/30, 16/30)$, se obtiene:

$$\mathcal{N}_3 = \mathcal{O}\left(R_4^{5+\frac{\ell-1}{k+1}}\right) = \mathcal{O}\left(R_4^{\frac{191}{41}}\right).$$

Reuniendo las estimaciones de $\mathcal{N}_1$, $\mathcal{N}_2$ y $\mathcal{N}_3$, se concluye:

$$\mathcal{N}(\lambda) = \frac{1}{4}\int_{\mathbb{R}^2} m_4(\vec{x})\chi_{R_4}(\vec{x})\,d\vec{x} + \mathcal{O}\left(R_4^{\frac{191}{41}}\right) = C_6\lambda^3 + \mathcal{O}\left(\lambda^{2+\frac{27}{82}}\right).$$

(*B*) El polinomio que define la multiplicidad de los autovalores es $m_5(x,y) = x^2y^2(x^2-y^2)^2/576$. Por tanto, siendo $R_5^2 = 4\lambda + 10$ y suponiendo $y > x$, se tiene por las simetrías de $m_5(\vec{x})$ para $x = 2u-1$ e $y = 2v-1$:

$$\mathcal{N}(\lambda) = \frac{1}{8}\sum_{\vec{x}\in\mathbb{O}^2} m_5(x,y)\chi_{R_5}(\vec{x}) = \sum_{1\le u\le \frac{R_5+\sqrt{2}}{2\sqrt{2}}}\ \sum_{v\in I_u} m(2u-1,2v-1), \qquad I_u := \left(u, \frac{\sqrt{R_5^2-(2u-1)^2}+1}{2}\right];$$

Aplicando (16) a la suma interior se obtiene:

$$\sum_{v\in I_u} m_5(2u-1,2v-1) = \psi\left(\frac{\sqrt{R_5^2-(2u-1)^2}+1}{2}\right) m_5\left(2u-1,\sqrt{R_5^2-(2u-1)^2}\right)$$
$$+\int_u^{\frac{\sqrt{R_5^2-(2u-1)^2}+1}{2}} m_5(2u-1,2v-1)\,dv + \int_u^{\frac{\sqrt{R_5^2-(2u-1)^2}+1}{2}} \frac{\partial m_5(2u-1,2v-1)}{\partial v}\psi(v)\,dv,$$

y sustituyendo en $\mathcal{N}(\lambda)$ se tiene la expresión $\mathcal{N}(\lambda) = \mathcal{N}_1 + \mathcal{N}_2 + \mathcal{N}_3$, donde:

$$\mathcal{N}_1 = \sum_{1\le u\le \frac{R_5+\sqrt{2}}{2\sqrt{2}}}\ \int_u^{\frac{\sqrt{R_5^2-(2u-1)^2}+1}{2}} m_5(2u-1,2v-1)\,dv,$$

$$\mathcal{N}_2 = \sum_{1\le u\le \frac{R_5+\sqrt{2}}{2\sqrt{2}}}\ \int_u^{\frac{\sqrt{R_5^2-(2u-1)^2}+1}{2}} \frac{\partial m_5(2u-1,2v-1)}{\partial v}\psi(v)\,dv,$$

$$\mathcal{N}_3 = \sum_{1\le u\le \frac{R_5+\sqrt{2}}{2\sqrt{2}}}\ \psi\left(\frac{\sqrt{R_5^2-(2u-1)^2}+1}{2}\right) m_5\left(2u-1,\sqrt{R_5^2-(2u-1)^2}\right).$$

Para el término $\mathcal{N}_1$ se aplica de nuevo (16), consiguiendo:

$$\mathcal{N}_1 = \int_1^{\frac{R_5+\sqrt{2}}{2\sqrt{2}}}\ \int_u^{\frac{\sqrt{R_5^2-(2u-1)^2}+1}{2}} m_5(2u-1,2v-1)\,du\,dv$$
$$-\int_1^{\frac{R_5+\sqrt{2}}{2\sqrt{2}}} \frac{2u-1}{\sqrt{R_5^2-(2u-1)^2}} m_5\left(2u-1,\sqrt{R_5^2-(2u-1)^2}\right)\psi(u)\,du.$$

Aprovechando una vez más que la integral de $\psi(x)$ es $\mathcal{O}(1)$ por el *Segundo Teorema del Valor Medio*, la segunda de las integrales de $\mathcal{N}_1$ puede acotarse así:

$$\left|\int_1^{\frac{R_5+\sqrt{2}}{2\sqrt{2}}} \frac{2u-1}{\sqrt{R_5^2-(2u-1)^2}} m_5\left(2u-1,\sqrt{R_5^2-(2u-1)^2}\right)\psi(u)\,du\right|$$
$$\ll \max_{[1,\frac{R_5+\sqrt{2}}{2\sqrt{2}}]} \frac{(2u-1)^3(R_5^2-(2u-1)^2)(R_5^2-2(2u-1)^2)^2}{\sqrt{R_5^2-(2u-1)^2}} \cdot \left|\int_\xi^\eta \psi(u)\,du\right| \ll R_5^8.$$

De esta forma, volviendo a tener en cuenta las simetrías de m_5 se satisface para $\vec{u} := (u,v)$:

$$\mathcal{N}_1 = \frac{1}{8}\int_{\mathbb{R}^2} m_5(2u-1,2v-1)\chi_{\frac{R_5+1}{2}}(\vec{u})\,d\vec{u} + \mathcal{O}(R_5^8) = \frac{1}{32}\int_{\mathbb{R}^2} m_5(x,y)\chi_{R_5}(\vec{x})\,d\vec{x} + \mathcal{O}(R_5^8).$$

Por otra parte, para el término $\mathcal{N}_2$ se procede de forma similar:

$$\mathcal{N}_2 = \sum_{1\le u\le \frac{R_5+\sqrt{2}}{2\sqrt{2}}}\ \int_u^{\frac{\sqrt{R_5^2-(2u-1)^2}+1}{2}} \frac{4}{576}(2u-1)^2(2v-1)((2u-1)^2-(2v-1)^2)((2u-1)^2-3(2v-1)^2)\psi(v)\,dv$$
$$\ll \sum_{1\le u\le \frac{R_5+\sqrt{2}}{2\sqrt{2}}} R_5^7\left|\int_\xi^\eta \psi(v)\,dv\right| \ll R_5^8.$$

Por último, para el término $\mathcal{N}_3$ se vuelve a recurrir a las series de Fourier $Q^{\pm}(x)$ utilizadas en (A) para obtener:

$$\sum_{|m|\leq M} a_m^- S(m) \leq \mathcal{N}_3 \leq \sum_{|m|\leq M} a_m^+ S(m),$$

donde, deshaciendo el cambio $x = 2u - 1$:

$$\begin{aligned} S(m) &:= \sum_{1\leq u\leq \frac{R_5+\sqrt{2}}{2\sqrt{2}}} m_5\left(2u-1, \sqrt{R_5^2-(2u-1)^2}\right) e^{\pi i m(1+\sqrt{R_5^2-(2u-1)^2})} \\ &= \frac{1}{576} \sum_{1\leq 2^\nu \leq \frac{R_5}{\sqrt{2}}} \sum_{\substack{\frac{R_5}{\sqrt{2}\cdot 2^{\nu+1}} < x \leq \frac{R_5}{\sqrt{2}\cdot 2^\nu} \\ x\in\mathbb{O}}} x^2(R_5^2-x^2)(R_5^2-2x^2)^2 e^{\pi i m(1+\sqrt{R_5^2-x^2})} \end{aligned}$$

La suma interior de $S(m)$, tomada con $x \in \mathbb{O}$ puede acotarse por la misma suma pero con $x \in \mathbb{Z}$, y a esta se le puede volver a aplicar (26) tomando en este caso $f(x) = m(1+\sqrt{R_5^2-x^2})/2$, de forma que $|f'(u)| = |m|x/(2\sqrt{R_5^2-x^2}) < |m|/(2\sqrt{2^{2\nu+1}-1})$ en el intervalo $R_5/\sqrt{2}\cdot(2^{-\nu-1}, 2^{-\nu}]$ y escogiendo un par de exponentes (k,ℓ) se tiene:

$$\begin{aligned} |\mathcal{N}_3| &\ll \left(|a_0^+| + |a_0^-|\right) R_5^9 \\ &+ \sum_{1\leq|m|\leq M} \left(|a_m^+| + |a_m^-|\right) R_5^8 \sum_{1\leq 2^\nu \leq \frac{R_5}{\sqrt{2}}} \frac{1}{2^{2\nu+1}} \left(1-\frac{1}{2^{2\nu+2}}\right)^2 \left(1-\frac{1}{2^{2\nu+3}}\right) \left(\frac{|m|}{2\sqrt{2^{2\nu+1}-1}}\right)^k \left(\frac{R_5}{2^{\nu+1}\sqrt{2}}\right)^\ell \\ &\ll M^{-1} R_5^9 \\ &+ R_5^{\ell+8} \sum_{1\leq|m|\leq M} |m|^{k-1} \sum_{1\leq 2^\nu \leq \frac{R_5}{\sqrt{2}}} \frac{1}{2^{2\nu+1}} \left(1-\frac{1}{2^{2\nu+2}}\right)^2 \left(1-\frac{1}{2^{2\nu+3}}\right) \left(\frac{1}{2\sqrt{2^{2\nu+1}-1}}\right)^k \left(\frac{1}{2^{\nu+1}\sqrt{2}}\right)^\ell \\ &\ll M^{-1} R_5^9 + M^k R_5^{\ell+8}. \end{aligned}$$

Al optimizar la estimación obtenida igualando los sumandos se tiene $M = R_5^{(1-\ell)/(1+k)}$. Así, usando una vez más el par $BA^3B(0,1) = (11/30, 16/30)$, se obtiene:

$$\mathcal{N}_3 = \mathcal{O}\left(R_5^{9+\frac{\ell-1}{k+1}}\right) = \mathcal{O}\left(R_5^{\frac{355}{41}}\right).$$

Reuniendo las estimaciones de $\mathcal{N}_1$, $\mathcal{N}_2$ y $\mathcal{N}_3$, se concluye:

$$\mathcal{N}(\lambda) = \frac{1}{32}\int_{\mathbb{R}^2} m_5(\vec{x})\chi_{R_5}(\vec{x})\,d\vec{x} + \mathcal{O}\left(R_5^{\frac{355}{41}}\right) = C_{10}\lambda^5 + \mathcal{O}\left(\lambda^{4+\frac{27}{82}}\right).$$

□

Antes de proseguir con el caso $n = 3$, es posible probar una fórmula para $r_2^{\mathbb{Z}}(k)$ [**?**]:

Lema 1.24 *Se tiene:*

$$r_2^{\mathbb{Z}}(k) = 4\delta(k) := 4 \sum_{\substack{d|k \\ d\equiv 1 \,(\mathrm{mod}\, 4)}} 1 - 4 \sum_{\substack{d|k \\ d\equiv 3 \,(\mathrm{mod}\, 4)}} 1.$$

Demostración. Sea $k = 2^\kappa k_1 k_3$, donde para p y q primos:

$$k_1 = \prod_{p\equiv 1 \,(\mathrm{mod}\, 4)} p^a, \qquad k_3 = \prod_{q\equiv 3 \,(\mathrm{mod}\, 4)} q^b.$$

Entonces $\delta(k) = \delta(k_1 k_3)$. Los divisores de $k_1 k_3$ vendrán dados por:

$$\prod \left(1 + p + \ldots + p^a\right) \prod \left(1 + q + \ldots + q^b\right),$$

y será de la forma $4m+1$ si contiene un número par de factores q y $4m+3$ en caso contrario. Por tanto, sustituyendo cada p por 1 y cada q por -1 se obtiene:

$$\delta(k) = \prod (a+1) \prod \frac{1+(-1)^b}{2}.$$

De aquí se deduce que si b es impar, entonces k_3 no es un cuadrado y $\delta(k) = 0$, mientras que si b es par, entonces k_3 es un cuadrado y $\delta(k) = d(k_1)$. Por tanto, para probar el enunciado hay que probar que $r_2^{\mathbb{Z}}(k) = 4d(k_1)$ cuando k_3 es un cuadrado y 0 en otro caso. Para ello, se descompone k utilizando los elementos de $\mathbb{Z}[i]$, llamados *enteros de Gauss*. Notando que $2 = -i(1+i)^2 = i^3(1+i)^2$, k puede escribirse como:

$$k = i^{3\kappa}(1+i)^{2\kappa} \prod (p_1 + p_2 i)^a (p_1 - p_2 i)^a \prod q^b, \qquad (p_1 \neq p_2,\ p = p_1^2 + p_2^2).$$

Esta factorización es única salvo producto por unidades y asociados de $\mathbb{Z}[i]$ ya que los *enteros de Gauss* forman un dominio euclídeo (cuyas unidades son $u = \pm 1, \pm i$) y sus elementos primos corresponden a $1+i$ y sus asociados, $p_1 \pm p_2 i$ divisores de $p \equiv 1 \pmod 4$ y los primos $q \equiv 3 \pmod 4$. El objetivo es encontrar el número de descomposiciones de k como $k = A^2 + B^2 = (A+Bi)(A-Bi)$, donde cada factor satisface:

$$A + Bi = u(1+i)^\kappa \prod (p_1 + p_2 i)^{a_1} (p_1 - p_2 i)^{a_2} \prod q^{b'}, \qquad A - Bi = \bar{u}(1-i)^\kappa \prod (p_1 - p_2 i)^{a_1} (p_1 + p_2 i)^{a_2} \prod q^{b'}.$$

Puesto que $|A+Bi| = |A-Bi| = A^2 + B^2$, al igualar ambos se llega a que $a_1 + a_2 = a$ y $2b' = b$. Con esto se observa que una condición necesaria para que $k = A^2 + B^2$ es que todos los exponentes b sean pares. Por otra parte, se tendrán $a+1$ elecciones de los exponentes a_1 y cuatro posibles elecciones de la unidad u. Por tanto, $r_2^{\mathbb{Z}}(k) = 4d(k_1)$ si todos los b son pares y 0 en caso contrario, lo que es equivalente a lo que se quería demostrar.□

Este resultado se puede emplear para probar los siguientes pasos previos [**?**] a la demostración del caso $n = 3$:

Lema 1.25 *Sean las cantidades para $N = 6, 7$:*

$$\mathcal{M}(R_N) := \sum_{\vec{n} \in \mathbb{B}^3_{R_N} \cap \mathbb{A}^3} 1, \qquad \mathcal{E}(R_N) := \mathcal{M}(R_N) - \frac{4\pi\kappa_N}{3} R_N^3,$$

donde $\mathbb{A} = \mathbb{Z}$ si $N = 6$, $\mathbb{A} = \mathbb{O}$ si $N = 7$, $\kappa_6 = 1$ y $\kappa_7 = 1/8$.

(*A*) *En cada caso, dado $\delta = R_N^{-c}$ con $0 < c < 1$ existe $R'_N \in (R_N - 2, R_N + 2)$ tal que:*

$$\mathcal{E}(R_N) = -\frac{\kappa_N R'_N}{\pi} \sum_{n=1}^{\infty} (-1)^{Nn} \frac{r_3^{\mathbb{Z}}(n)}{n'} \eta(\delta\sqrt{n'}) \cos\left(2\pi R'_N \sqrt{n'}\right) + \mathcal{O}\left(\delta R_N^{2+\varepsilon}\right),$$

siendo $n' = n$ si $N = 6$, $n' = n/4$ si $N = 7$, $\varepsilon > 0$ y $\eta \in C_0^\infty(-1,1)$ una función par con $\eta(0) = 1$ y $\mathcal{F}[\eta(\delta\|\vec{x}\|)] > 0$ para todo $\vec{x}$.

(*B*) $\mathcal{E}(R_N) = \mathcal{O}\left(R_N^{37/25+\varepsilon}\right)$.

Demostración.

(*A*) Sean $0 < \varepsilon < 1$ arbitrariamente pequeño y $\phi_\delta(\cdot) := \mathcal{F}[\eta(\delta\|\cdot\|)]$. Como $\eta \in C_0^\infty$, para $\xi \to \infty$ se cumple para m grande que $\mathcal{F}[\eta](\xi) = \mathcal{O}(|\xi|^{-m})$. Por tanto, realizando el cambio $\vec{x} = \vec{y}/\delta$:

$$\phi_\delta(\vec{\xi}) = \int_{\mathbb{R}^3} \eta(\delta\|\vec{x}\|) e^{-2\pi i \vec{x}\cdot\vec{\xi}}\, d\vec{x} = \delta^{-1} \int_{\mathbb{R}^3} \eta(\|\vec{y}\|) e^{-2\pi i \vec{y}\cdot\vec{\xi}/\delta}\, d\vec{y} = \delta^{-1}\mathcal{O}\left(\delta^m \|\vec{\xi}\|^{-m}\right),$$

lo que implica para $k := m\varepsilon - 1$, teniendo en cuenta que $\mathcal{F}[\phi_\delta](0) = \eta(0) = 1$ y $\eta \in C_0^\infty$:

$$\int_{\|\vec{\xi}\| > \delta^{1-\varepsilon}} \phi_\delta(\vec{\xi})\, d\vec{\xi} = \mathcal{O}\left(\delta^{m-1-m(1-\varepsilon)}\right) = \mathcal{O}(\delta^k),$$

$$\int_{\|\vec{\xi}\| \leq \delta^{1-\varepsilon}} \phi_\delta(\vec{\xi})\, d\vec{\xi} = \int_{\mathbb{R}^3} \phi_\delta(\vec{\xi})\, d\xi - \int_{\|\vec{\xi}\| > \delta^{1-\varepsilon}} \phi_\delta(\vec{\xi})\, d\vec{\xi} = 1 + \mathcal{O}(\delta^k).$$

Sea χ_{R_N} la función característica de $\mathbb{B}^3_{R_N}$ y sean $R_{N,1} = R_N - 2\delta^{1-\varepsilon}$ y $R_{N,2} = R_N + 2\delta^{1-\varepsilon}$. Puesto que $R_{N,1} < R_N < R_{N,2}$, sus funciones características respectivas verifican que $\chi_{R_{N,1}}(\vec{x}-\vec{\xi}) \leq \chi_{R_N}(\vec{x}) \leq \chi_{R_{N,2}}(\vec{x}-\vec{\xi})$ para todo $\vec{x}$ siempre que $\|\vec{\xi}\| \leq \delta^{1-\varepsilon}$. Esto implica que para $j = 1, 2$:

$$\begin{aligned}(\phi_\delta * \chi_{R_{N,j}})(\vec{x}) &= \int_{\mathbb{R}^3} \phi_\delta(\vec{\xi})\chi_{R_{N,j}}(\vec{x}-\vec{\xi})\,d\xi \\ &= \int_{\|\vec{\xi}\|\leq\delta^{1-\varepsilon}} \phi_\delta(\vec{\xi})\chi_{R_{N,j}}(\vec{x}-\vec{\xi}) + \int_{\|\vec{\xi}\|>\delta^{1-\varepsilon}} \phi_\delta(\vec{\xi})\chi_{R_{N,j}}(\vec{x}-\vec{\xi})\,d\xi \begin{cases} \leq \chi_{R_N}(\vec{x}) + \mathcal{O}(\delta^k) & \text{si } j=1 \\ \geq \chi_{R_N}(\vec{x}) + \mathcal{O}(\delta^k) & \text{si } j=2 \end{cases}\end{aligned}$$

Uniendo ambos casos, se deduce que $\mathcal{O}(\delta^k)+(\phi_\delta * \chi_{R_{N,1}})(\vec{n}) \leq \chi_{R_N}(\vec{n}) \leq (\phi_\delta * \chi_{R_{N,2}})(\vec{n}) + \mathcal{O}(\delta^k)$ para $\vec{n} \in \mathbb{A}^3$, luego existe R'_N con $|R'_N - R_N| < 2\delta^{1-\varepsilon}$ tal que usando la estimación de ϕ_δ se llega a:

$$\begin{aligned}\mathcal{M}(R_N) &= \sum_{\vec{n}\in\mathbb{B}^3_{100R_N}\cap\mathbb{A}^3} \chi_{R_N}(\vec{n}) = \sum_{\vec{n}\in\mathbb{B}^3_{100R_N}\cap\mathbb{A}^3} (\phi_\delta * \chi_{R'_N})(\vec{n}) + \sum_{\vec{n}\in\mathbb{B}^3_{100R_N}\cap\mathbb{A}^3} \mathcal{O}(\delta^k) \\ &= \sum_{\vec{n}\in\mathbb{A}^3} (\phi_\delta * \chi_{R'_N})(\vec{n}) + \mathcal{O}\left(\sum_{\|\vec{n}\|\geq 100R_N} (\phi_\delta * \chi_{R'_N})(\vec{n})\right) + \mathcal{O}(\delta^k R_N^3) = \sum_{\vec{n}\in\mathbb{A}^3} (\phi_\delta * \chi_{R'_N})(\vec{n}) + \mathcal{O}(\delta^k R_N^3),\end{aligned}$$

ya que:

$$\sum_{\|\vec{n}\|\geq 100R_N} (\phi_\delta * \chi_{R'_N})(\vec{n}) = \sum_{\|\vec{n}\|\geq 100R_N} \int_{\|\vec{t}\|<R'_N} \phi_\delta(\vec{n}-\vec{t})\,d\vec{t} = \mathcal{O}\left(\delta^{m-1}R_N^3 \sum_{\|\vec{n}\|\geq 100R_N} \|\vec{n}\|^{-m}\right) = \mathcal{O}\left(\delta^{m-1}R_N^3\right).$$

El objetivo es aplicar (17) a la suma de $\mathcal{M}(R_N)$. Para poder hacerlo, en el caso particular $N = 7$ es necesario expresar la suma en $\mathbb{O}^3$ como una suma en $\mathbb{Z}^3$. Por tanto, si $\vec{n} = (n_1, n_2, n_3)$ y $n := n_1^2 + n_2^2 + n_3^2 = \|\vec{n}\|^2$, se puede deducir agrupando los casos $N = 6$ y $N = 7$:

$$\sum_{\vec{n}\in\mathbb{A}^3} (\phi_\delta * \chi_{R'_N})(\vec{n}) = \kappa_N \sum_{\vec{n}\in\mathbb{Z}^3} \mathcal{F}[\phi_\delta * \chi_{R'_N}](\vec{n}')e^{i\pi(n_1+n_2+n_3)N} = \kappa_N \sum_{\vec{n}\in\mathbb{Z}^3} (-1)^{Nn}\eta(\delta\|\vec{n}'\|)\mathcal{F}[\chi_{R'_N}](\vec{n}'),$$

donde $\vec{n}' = \vec{n}$ si $N = 6$ y $\vec{n}' = \vec{n}/2$ si $N = 7$. A continuación, se evalúa la transformada de Fourier de $\chi_{R'_N}(\vec{n}')$. En general, si f es una función *radial*, es decir, $f(\vec{x}) = g(\|\vec{x}\|)$, entonces su transformada de Fourier verifica que $\mathcal{F}[f](\vec{\xi}) = \mathcal{F}[f](0, 0, \|\vec{\xi}\|)$. Puesto que $\chi_{R'_N}$ es una función radial por definición, se deduce para $\vec{n}' \neq \vec{0}$:

$$\begin{aligned}\mathcal{F}[\chi_{R'_N}](\vec{n}') = \mathcal{F}[\chi_{R'_N}](0, 0, \|\vec{n}'\|) &= \int_0^{R'_N}\int_{\varphi=0}^{2\pi}\int_{\theta=0}^{\pi} e^{-2\pi i r\|\vec{n}'\|\cos\theta} r^2 \operatorname{sen}\theta\,dr\,d\theta\,d\varphi \\ &= \frac{1}{\pi\|\vec{n}'\|^2}\cdot\left(-R'_N\cos(2\pi R'_N\|\vec{n}'\|) + \frac{\operatorname{sen}(2\pi R'_N\|\vec{n}'\|)}{2\pi\|\vec{n}'\|}\right) = -\frac{R'_N}{\pi\|\vec{n}'\|^2}\cos(2\pi R'_N\|\vec{n}'\|) + \mathcal{O}\left(\frac{1}{\|\vec{n}'\|^3}\right).\end{aligned}$$

Por otra parte:

$$\mathcal{F}[\chi_{R'_N}](\vec{0}) = \int_{\mathbb{R}^3} \chi_{R'_N}(\vec{x})\,d\vec{x} = |\mathbb{B}^3_{R'_N}| = \frac{4\pi}{3}(R'_N)^3.$$

Sustituyendo estas expresiones en $\mathcal{M}(R_N)$ se obtiene:

$$\begin{aligned}\mathcal{M}(R_N) = \frac{4\pi\kappa_N}{3}(R'_N)^3 - \frac{\kappa_N R'_N}{\pi}\sum_{\vec{n}\in\mathbb{Z}^3\setminus\{\vec{0}\}} (-1)^{Nn}\frac{\eta(\delta\|\vec{n}'\|)}{\|\vec{n}'\|^2}\cos(2\pi R'_N\|\vec{n}'\|) \\ + \mathcal{O}\left(\sum_{\vec{n}\in\mathbb{Z}^3\setminus\{\vec{0}\}} \frac{\eta(\delta\|\vec{n}'\|)}{\|\vec{n}'\|^3}\right) + \mathcal{O}\left(\delta^k R_N^3\right).\end{aligned}$$

Así, transformando las sumas con $\vec{n}$ en función de sus módulos, la expresión de $\mathcal{E}(R_N)$ queda:

$$\begin{aligned}\mathcal{E}(R_N) = \frac{4\pi\kappa_N}{3}\left((R'_N)^3 - R_N^3\right) - \frac{\kappa_N R'_N}{\pi}\sum_{n=1}^{\infty}(-1)^{Nn}\frac{r_3^{\mathbb{Z}}(n)}{n'}\eta(\delta\sqrt{n'})\cos(2\pi R'_N\sqrt{n'}) \\ + \mathcal{O}\left(\sum_{n=1}^{\infty}\frac{r_3^{\mathbb{Z}}(n)}{(n')^{3/2}}\eta(\delta\sqrt{n'})\right) + \mathcal{O}\left(\delta^k R_N^3\right).\end{aligned}$$

A partir de aquí pueden hacerse algunas simplificaciones. En primer lugar, dado que $\delta = R^{-c}$ con $0 < c < 1$, es posible deducir empleando la identidad $a^3 - b^3 = (a-b)(a^2+ab+b^2)$:

$$\frac{4\pi\kappa_N}{3}\left((R'_N)^3 - R_N^3\right) \ll (R_N + 2\delta^{1-\varepsilon})^3 - R_N^3 = 2\delta^{1-\varepsilon}\left(3R_N^2 + 6R_N\delta^{1-\varepsilon} + 4\delta^{2-2\varepsilon}\right) \ll \delta^{1-\varepsilon}R_N^2 \ll \delta R_N^{2+\varepsilon}.$$

Por otra parte, gracias al Lema 1.24 se cumple que $r_2^{\mathbb{Z}}(n) \ll d(n) = \mathcal{O}(n^{\varepsilon})$, por lo que:

$$r_3^{\mathbb{Z}}(n) = \sum_{m^2\leq n} r_2^{\mathbb{Z}}(n-m^2) = \sum_{m^2\leq n} \mathcal{O}\left(\left(n-m^2\right)^{\varepsilon}\right) = \mathcal{O}\left(n^{\frac{1}{2}+\varepsilon}\right).$$

Teniendo esto en cuenta y que $\eta \in C_0^{\infty}(-1,1)$, entonces los términos de las sumas en $\mathcal{E}(R_N)$ contribuirán a la misma siempre que $\delta\sqrt{n'} < 1$. En particular, para la suma del término de error se tendrá:

$$\sum_{n=1}^{\infty} \frac{r_3^{\mathbb{Z}}(n)}{(n')^{3/2}}\eta(\delta\sqrt{n'}) \ll \sum_{n<\delta^{-2}} \frac{r_3^{\mathbb{Z}}(n)}{n^{3/2}} \ll \sum_{n<\delta^{-2}} \frac{1}{n^{1-\varepsilon}} \ll \log\delta^{-2} \ll \delta^{-2\varepsilon}.$$

Al sustituir estas simplificaciones en $\mathcal{E}(R_N)$, su expresión queda con los términos de error $\mathcal{O}(\delta R_N^{2+\varepsilon})$, $\mathcal{O}(\delta^k R_N^3)$ y $\mathcal{O}(\delta^{-2\varepsilon})$. Puesto que $k = m\varepsilon - 1$, el mayor de ellos es el primero tomando m suficientemente grande y así se concluye el enunciado.

(*B*) Para $n = n_1^2 + n_2^2 + n_3^2$ con $0 \leq n_3 \leq n_2 \leq n_1$, sea la suma trigonométrica:

$$S_M = \sum_{n\leq M^2} r_3^{\mathbb{Z}}(n) e^{2\pi i R'_N\sqrt{n'}} \ll M^2 \sum_{M/\sqrt{3}\leq n_1\leq M} e^{2\pi i R'_N\sqrt{(n'_1)^2+(n'_2)^2+(n'_3)^2}}.$$

La idea es aplicar (26) para lograr la estimación del enunciado. Fijando los parámetros n_2 y n_3, sea $f(n_1) = R'_N\sqrt{(n'_1)^2+(n'_2)^2+(n'_3)^2}$. Entonces su derivada verifica:

$$f'(n_1) = \frac{R'_N n'_1}{\sqrt{(n'_1)^2+(n'_2)^2+(n'_3)^2}} \sim R'_N.$$

Aplicando el par de exponentes $A^2B(0,1) = (1/14, 11/14)$, se deduce que $S_M \ll M^{2+11/14}(R'_N)^{1/14}$. El último paso es expresar $\mathcal{E}(R_N)$ en términos de S_M y aplicar su estimación junto con (14):

$$\begin{aligned}\mathcal{E}(R_N) &\ll R'_N \sum_{n\leq\delta^{-2}} \frac{r_3^{\mathbb{Z}}(n)}{n}\cos\left(2\pi R'_N\sqrt{n'}\right) + \delta R_N^{2+\varepsilon} = R'_N\cdot\mathrm{Re}\left(\sum_{n\leq\delta^{-2}} \frac{r_3^{\mathbb{Z}}(n)}{n} e^{2\pi i R'_N\sqrt{n'}}\right) + \delta R_N^{2+\varepsilon} \\ &= R'_N\left(\delta^2 S_{\delta^{-1}} + \mathcal{O}(1) + \int_1^{\delta^{-2}} S_{\sqrt{t}}\frac{dt}{t^2}\right) + \delta R_N^{2+\varepsilon} \ll \delta^{-\frac{11}{14}}(R'_N)^{\frac{15}{14}} + \delta R_N^{2+\varepsilon}.\end{aligned}$$

Al optimizar la cota igualando ambos sumandos se obtiene $\delta = (R'_N)^{3/5}R_N^{-(2+\varepsilon)14/25}$ y al sustituir, teniendo en cuenta que $R'_N \ll R_N^{1+\varepsilon}$, se concluye que $\mathcal{E}(R_N) \ll R_N^{37/25+17\varepsilon/25} \leq R_N^{37/25+\varepsilon}$. □

Con este resultado, el caso $n = 3$ se vuelve un cálculo directo:

Proposicion 1.26 (Chamizo-G.) *Para $n = 3$, existen constantes positivas C_{15} y C_{21} tales que en $\mathbf{SO}(6)$ y $\mathbf{SO}(7)$ se verifica respectivamente:*

$$\mathcal{N}(\lambda) = C_{15}\lambda^{15/2} + \mathcal{O}(\lambda^{15/2-3/4}\log\lambda), \qquad \mathcal{N}(\lambda) = C_{21}\lambda^{21/2} + \mathcal{O}(\lambda^{21/2-3/4}\log\lambda).$$

Demostración. Recuperando la fórmula del final del Paso 2 de la Sección 2, válida en general, para $n = 3$:

$$\mathcal{N}(\lambda) = C_{1,N}P_0\sum_{k\leq R_N^2} k^{\frac{d-3}{2}} r_3^{\mathbb{A}}(k) + \mathcal{O}\left(R_N^{d-\frac{3}{2}}\log R_N\right).$$

Gracias al Lema 1.25, se ha probado que existe un número $\alpha < 3/2$ tal que:

$$\sum_{k\leq R_N^2} r_3^{\mathbb{A}}(k) = \frac{4\pi\kappa_N}{3}R_N^3 + \mathcal{O}(R_N^{\alpha}).$$

Por tanto, basta aplicar (14) para obtener:

$$\mathcal{N}(\lambda) = C_{1,N}P_0\left[\left(\sum_{k\leq R_N^2} r_3^{\mathbb{A}}(k)\right)R_N^{d-3} - \frac{d-3}{2}\int_1^{R_N^2}\left(\sum_{k\leq t} r_3^{\mathbb{A}}(k)\right)\cdot t^{\frac{d-3}{2}-1}\,dt\right] + \mathcal{O}\left(R_N^{d-\frac{3}{2}}\log R_N\right)$$
$$= \frac{4\pi\kappa_N}{d}C_{1,N}P_0R_N^d + \mathcal{O}\left(R_N^{d+\alpha-3}\right) + \mathcal{O}\left(R_N^{d-\frac{3}{2}}\log R_N\right).$$

Puesto que $\alpha < 3/2$, el segundo término de error es mayor que el primero y al ser $R_N \sim \lambda^{1/2}$, se concluye el enunciado. □

Capítulo 2

Una prueba simple del Teorema de los Números Primos en Progresiones Aritméticas

§1. El Teorema de los Números Primos, sus diferentes pruebas y su extensión a las progresiones aritméticas

De entre los resultados clásicos más importantes de la *Teoría de Números*, el llamado *Teorema de los Números Primos* ha supuesto todo un hito en cuanto a la influencia que ha tenido en gran cantidad de resultados posteriores y un gran desafío dentro del mundo matemático para encontrar una prueba que lo sustentara. Todo ello se originó en un intento por describir una ley que explicara la aparentemente aleatoria distribución de los números primos dentro de los números naturales, una vez que Euclides (300 a.C.) probara la existencia de infinitos [**?**]. A partir de aquí, se ha intentado describir tal comportamiento de dos formas: o bien a través de una fórmula que originara una infinidad de ellos o bien a través de leyes que describieran el comportamiento general de los mismos. En esta última línea, se podría decir que el primer *Teorema de los Números Primos* fue enunciado de forma conjetural por Legendre en 1798 en base a una tabla de valores. De forma general, tanto Legendre como matemáticos posteriores sostuvieron que si $\pi(x)$ es la función contadora de primos hasta un número real x, se tenía para cierta constante A (diferente según los autores):

$$\pi(x) \sim \frac{x}{\log x - A},$$

siempre que x recorriera un rango específico. De hecho, lo que ocurre es que para cualquier constante A, este enunciado es equivalente al *Teorema de los Números Primos*, que afirma:

$$\pi(x) \sim \frac{x}{\log x}.$$

Como se ha comentado, no ha existido un único enunciado para el *Teorema de los Números Primos* y se ha buscado establecer equivalencias entre ellos con el fin de tener varias opciones para investigar una prueba o para deducir otros resultados concernientes a las funciones involucradas. Dichas equivalencias han sido constatadas por matemáticos como Tchebychev o Landau. De entre ellas, las más clásicas y que serán útiles en este Capítulo son las siguientes:

$$\pi(x) \sim \frac{x}{\log x} \quad \Leftrightarrow \quad \psi(x) := \sum_{n \leq x} \Lambda(n) \sim x \quad \Leftrightarrow \quad M(x) := \sum_{n \leq x} \mu(n) = o(x).$$

No fue hasta 1896 cuando el teorema fue probado de forma independiente por los matemáticos Hadamard [**?**] y de la Vallée-Poussin [**?**]. El fundamento de dicha prueba está íntimamente ligado a la mundialmente conocida y aún no demostrada o refutada *Hipótesis de Riemann*. Presentada por Riemann en su famosa memoria [**?**], sostiene que la función:

$$\zeta(s) := \sum_{n=1}^{\infty} \frac{1}{n^s}$$

posee sus ceros no triviales como función de la variable compleja s en la recta $\mathrm{Im}(s) = 1/2$. En la prueba de Hadamard y de la Vallée-Poussin se utiliza, entre otros aspectos, el hecho de que $\zeta(s) \neq 0$ para todo $s = 1 + it$ con

$|t| > 0$. Esto unido a técnicas de integración de contorno en regiones que rodean ceros triviales de $\zeta(s)$ y la región de convergencia absoluta de la propia función deriva en una prueba de carácter analítico que supuso un triunfo ya que por primera vez existía una explicación fundamentada del comportamiento de los primos.

Una vez que se tuvo el comportamiento asintótico, el siguiente paso consistió en mejorar el término de error que se produce al comparar $\pi(x)$ con $x/\log x$, para lo cual de la Vallée-Poussin pudo deducir casi al mismo tiempo un término de error más preciso y reducido llegando a concluir que para una constante absoluta $C > 0$ se tiene:

$$\psi(x) = x + \mathcal{O}\left(xe^{-C\sqrt{\log x}}\right).$$

El poder afinar de forma progresiva el término de error supone aplicar integración de contorno en diferentes dominios, en los cuales la dificultad radica en ver que no contengan ceros de $\zeta(s)$. En el período comprendido entre 1958 y 1965, los matemáticos Vinogradov [**?**] y Korobov [**?**] probaron la mejor estimación conocida hasta el momento, que corresponde a la asintótica:

$$\psi(x) = x + \mathcal{O}\left(xe^{-C\log^{\frac{3}{5}} x(\log\log x)^{-\frac{1}{5}}}\right),$$

para $x \geq 3$ y $C > 0$ otra constante absoluta. El fundamento de la prueba de esta versión radica en cotas más finas para $\zeta(s)$ en torno a la recta $\mathrm{Re}(s) = 1$ gracias a un resultado propio de Vinogradov [**?**], [**?**] acerca de la estimación de sumas exponenciales.

Paralelamente a todo este desarrollo histórico, durante un período de tiempo surgió una corriente que, dada la complejidad de las pruebas que se han mencionado anteriormente, de carácter analítico, buscó el ver si existían pruebas llamadas elementales, las cuales se fundamentaran en una manipulación de las propias sumas involucradas, sin recurrir al uso de técnicas propias de otros campos como la variable compleja, reduciéndose a utilizar aspectos y propiedades muy básicos. En este sentido, a pesar del escepticismo que había en torno a dicha existencia de pruebas elementales para grandes resultados como este, en 1949 Erdös [**?**] y Selberg [**?**] publicaron la primera prueba elemental del *Teorema de los Números Primos* en su forma $\psi(x) \sim x$, cuya demostración parte de la idea fundamental dada por una identidad que demostró Selberg:

$$\sum_{p\leq x} \log^2 p + \sum_{pq\leq x} \log p \log q = 2x\log x + \mathcal{O}(x).$$

La aparición de una prueba de estas características hizo despertar todo un interés por la persecución de más pruebas elementales para otros resultados. Desafortunadamente, el precio que hay que pagar en cada una de estas pruebas es que los argumentos elementales hacen que las demostraciones sean mucho más largas e incluso tediosas en comparación al uso de otros métodos más analíticos. Es por ello que esta tendencia no gozó de una popularidad duradera en el tiempo.

A partir de la identidad de Selberg es posible deducir la desigualdad:

$$|M(x)|\log x < \sum_{n\leq x} \left|M\left(\frac{x}{n}\right)\right| + \mathcal{O}\left(x\log\log 3x\right),$$

algo que permitió en 1955 a Postnikov y Romanov [**?**] probar igualmente de forma elemental que $M(x) = o(x)$. A partir de estas pruebas, se refinaron los métodos utilizados por Erdös y Selberg, y así, tomándolos como referencia, surgieron otras pruebas algo menos elementales como la de Bombieri [**?**] y Wirsing [**?**] en 1962-64:

$$\psi(x) = x + \mathcal{O}\left(x\log^{-A} x\right),$$

para $A > 0$ constante arbitraria; o la de Diamond y Steinig [**?**] en 1970:

$$|\psi(x) - x| \leq xe^{-\log^{\frac{1}{7}} x(\log\log x)^{-2}},$$

para todo $x \geq e^{e^{100}}$. Aunque, como se ha comentado, en todas estas pruebas posteriores el argumento se vuelve menos elemental si se compara con pruebas como la de Selberg, como contrapartida ofrecen más información acerca del término de error.

Como alternativa a las pruebas elementales, existe una vía intermedia entre ellas y las pruebas analíticas. Más concretamente, ¿existiría una forma de encontrar una prueba analítica pero lo suficientemente simple como para que pudiera ser considerada en cierto sentido elemental? Iwaniec publicó en su libro *Analitic Number Theory*, en coautoría con Kowalski, una versión de la prueba del *Teorema de los Números Primos* en su forma:

$$M(x) = x + \mathcal{O}\left(x \log^{-A} x\right).$$

En dicha prueba, Iwaniec parte de eliminar el polo que tiene la función $\zeta(s)$ en $s = 1$ para buscar una serie de acotaciones superiores e inferiores de tal manera que al usar una fórmula estándar del cálculo diferencial y un resultado de integración compleja en una región muy sencilla, logra probar dicho enunciado. Así se logra una extensión más corta y un argumento más simple en comparación con otras demostraciones tanto analíticas como elementales. Aunque el punto de partida de Iwaniec sea eliminar el polo de $\zeta(s)$, este paso inicial no es algo crucial (de hecho, Cohen escribe una versión de la prueba sin hacerlo [**?**]) aunque facilita la construcción de las acotaciones posteriores. Si se observa la prueba de en sí, la conclusión a la que se llega es un comportamiento asintótico que da lugar a un término de error que obviamente no corresponde a la mejor cota que se conoce hoy en día, pero ofrece un grado de simplificación tal que podría ser considerada una prueba elemental. Este será el punto de referencia para el desarrollo de este Capítulo.

Una vez que se conoce el comportamiento asintótico en los primos, el siguiente objetivo es considerar qué ocurre si en lugar de seleccionarlos todos, se toman únicamente aquellos que estén en cierta progresión aritmética dada, es decir, aquellos que cumplan $p \equiv a \pmod{q}$, siendo a y q enteros positivos cualesquiera. El resultado, una vez que se aplican ideas análogas a las que han conducido hacia el *Teorema de los Números Primos* tanto en sus argumentos analíticos como elementales, es el *Teorema de los Números Primos en Progresiones Aritméticas*. Más concretamente, es posible deducir que cantidades como:

$$\sum_{\substack{p \leq x \\ p \equiv a \pmod{q}}} 1, \qquad \sum_{\substack{n \leq x \\ n \equiv a \pmod{q}}} \Lambda(n);$$

tienen para cada a y q fijados y coprimos desarrollos asintóticos equivalentes como

$$\frac{\mathrm{Li}(x)}{\varphi(q)} + \mathcal{O}\left(xe^{-C\sqrt{\log x}}\right) \quad \left[\mathrm{Li}(x) := \int_1^x \frac{dt}{\log t}\right], \qquad \frac{x}{\varphi(q)} + \mathcal{O}\left(xe^{-C\sqrt{\log x}}\right).$$

Los desarrollos pueden afinarse introduciendo nuevos conceptos para obtener estimaciones analíticas más complejas [**?**].

A priori, el comportamiento asintótico de los primos en progresiones aritméticas puede no ser similar, ya que se está considerando un subconjunto muy concreto del conjunto de todos los primos. Además, el hecho de que se seleccione tal subconjunto debe verse intuitivamente reflejado en dicho comportamiento. Por tanto, de aquí es posible plantearse las siguientes cuestiones:

- ¿De qué manera pueden seleccionarse los primos que cumplan la correspondiente condición $p \equiv a \bmod q$?
- Dados cualesquiera a y q, ¿es posible encontrar una infinidad de primos sobre los que se pueda estudiar un comportamiento asintótico?
- Una vez hallados tales primos, ¿cuál es el comportamiento asintótico?

A lo largo de este Capítulo se recorrerán todos los requisitos y herramientas necesarios para dar respuesta a cada una de las cuestiones planteadas, llegándose a probar una versión del *Teorema de los Números Primos en Progresiones Aritméticas* acorde con las ideas de Iwaniec en su prueba del *Teorema de los Números Primos*.

§2. Los caracteres y funciones L de Dirichlet y el Teorema de Dirichlet

Para poder seleccionar aquellos primos p que verifican la condición $p \equiv a \bmod q$, se introducen las siguientes herramientas:

Definición 2.1 *Un carácter de Dirichlet módulo q es una función aritmética $\chi : \mathbb{Z} \longrightarrow \mathbb{C}$ que satisface las siguientes propiedades:*

(A) $\chi(n) = \chi(n+q)$ *para todo entero n.*

(B) $\chi(n) = 0$ *si y solo si* $\operatorname{mcd}(n,q) > 1$.

(C) $\chi(mn) = \chi(m)\chi(n)$ *para cualesquiera enteros m y n.*

El *Teorema de Euler-Fermat* [**?**] sostiene que $a^{\varphi(q)} \equiv 1 \,(\mathrm{mod}\, q)$ siempre que a sea coprimo con q. Gracias a esto y a la condición (C), se deduce que $1 = \chi(1) = \chi(a^{\varphi(q)}) = \chi(a)^{\varphi(q)}$ para todo carácter χ. Entonces $\chi(a)$ es una raíz $\varphi(q)$-ésima de la unidad. Además, dada una raíz primitiva de $(\mathbb{Z}/q\mathbb{Z})^*$, es posible asociarle cada una de las $\varphi(q)$-ésimas raíces de la unidad, por lo que existen $\varphi(q)$ caracteres de Dirichlet módulo q. De entre ellos, uno poseerá especial importancia. Asociando a la raíz primitiva de $(\mathbb{Z}/q\mathbb{Z})^*$ la raíz de la unidad 1, se obtiene el llamado *carácter principal* χ_0, que verifica $\chi_0(n) = 1$ para todo n coprimo con q.

De la definición pueden deducirse nuevas propiedades de los caracteres de Dirichlet módulo q:

Proposicion 2.2 *(Relaciones de ortogonalidad) Se tiene:*

(A) $$\sum_{a \,(\mathrm{mod}\, q)} \chi(a) = \begin{cases} \varphi(q) & \text{si } \chi = \chi_0, \\ 0 & \text{si } \chi \neq \chi_0. \end{cases}$$

(B) *Si $\overline{\chi}$ es el caracter conjugado de χ, se verifica:*

$$\frac{1}{\varphi(q)} \sum_{\chi \,(\mathrm{mod}\, q)} \chi(n)\overline{\chi}(a) = \begin{cases} 1 & \text{si } n \equiv a \,(\mathrm{mod}\, q), \\ 0 & \text{en otro caso.} \end{cases}$$

En particular:

$$\sum_{\chi \,(\mathrm{mod}\, q)} \chi(n) = \begin{cases} \varphi(q) & \text{si } n \equiv 1 \,(\mathrm{mod}\, q), \\ 0 & \text{en otro caso.} \end{cases}$$

Demostración.

(A) Denotamos por S a la suma en cuestión. Si $\chi = \chi_0$, entonces $\chi(a) = 1$ para todo a coprimo con q y $\chi(a) = 0$ en cualquier otro caso, por lo que:

$$S = \sum_{\substack{1 \leq a \leq q \\ \operatorname{mcd}(a,q)=1}} 1 = \varphi(q).$$

Si $\chi \neq \chi_0$, entonces existe a' coprimo con q tal que $\chi(a') \neq 1$. Como a recorre los valores de 1 a q, así lo hace también $b = aa'$ reduciendo módulo q. Por tanto:

$$\chi(a')S = \sum_{\substack{1 \leq a \leq q \\ \operatorname{mcd}(a,q)=1}} \chi(a)\chi(a') = \sum_{\substack{1 \leq a \leq q \\ \operatorname{mcd}(a,q)=1}} \chi(aa') = \sum_{\substack{1 \leq b \leq q \\ \operatorname{mcd}(a,q)=1}} \chi(b) = S.$$

Como $\chi(a') \neq 1$, se concluye que $S = 0$.

(B) Si a no es coprimo con q, entonces $\chi(a) = 0$. Por tanto, se pueden tomar únicamente y sin pérdida de generalidad los $\varphi(q)$ números a coprimos con q. Considerando también los $\varphi(q)$ caracteres de Dirichlet módulo q, sea $A = (a_{ij})_{\varphi(q)\times\varphi(q)}$ la matriz tal que $a_{ij} = \chi_i(a_j)$. Entonces al aplicar (A), la matriz $B = A\overline{A}^t$ cumple:

$$b_{ij} = \sum_{k=0}^{\varphi(q)-1} \chi_i(a_k)\overline{\chi_j}(a_k) = \sum_{k=0}^{\varphi(q)-1} (\chi_i\overline{\chi_j})(a_k) = \begin{cases} \varphi(q) & \text{si } \chi_i\overline{\chi_j} = \chi_0, \\ 0 & \text{en otro caso.} \end{cases}$$

Puesto que $\chi_i\overline{\chi_j} = \chi_0$ si y solo si $i = j$, entonces $b_{ij} = \varphi(q)$ si $i = j$ y 0 en otro caso. Esto implica que $A\overline{A}^t = \varphi(q)I$. Utilizando el hecho de que A conmuta con su matriz inversa, entonces $C = \overline{A}^t A = A\overline{A}^t = \varphi(q)I$ y cada entrada de C verifica:

$$c_{ij} = \sum_{k=0}^{\varphi(q)-1} \overline{\chi_k}(a_i)\chi_k(a_j) = \begin{cases} \varphi(q) & \text{si } a_i = a_j, \\ 0 & \text{en otro caso.} \end{cases}$$

Teniendo en cuenta que si $a \equiv b \pmod q$ entonces $\chi(a) = \chi(b)$ para todo χ, se verifica la primera identidad del enunciado y aplicando la misma para $a = 1$ se concluye la segunda identidad. □

Las relaciones de ortogonalidad que se acaban de probar muestran la forma en la que se pueden seleccionar los primos $p \equiv a \pmod q$. Esto resuelve la primera cuestión planteada al final de la Sección 1. El objetivo siguiente es probar la existencia de infinitos primos en una progresión aritmética $a + nq$ con $n \in \mathbb{N}$. Para lograrlo, los caracteres de Dirichlet aparecerán en ciertas series cuyo comportamiento se analiza a continuación:

Proposicion 2.3 *(Sumas que involucran caracteres de Dirichlet) Sea χ un caracter de Dirichlet no principal y sea $f(x)$ una función no negativa tal que $f'(x)$ es negativa y continua para $x \geq x_0$. Entonces para $y \geq x \geq x_0$ se tiene:*

$$\sum_{x<n\leq y} \chi(n)f(n) = \mathcal{O}(f(x)).$$

Si además $\lim_{x\to\infty} f(x) = 0$, la serie total es convergente y su suma parcial verifica el siguiente comportamiento asintótico:

$$\sum_{n\leq x} \chi(n)f(n) = \sum_{n=1}^{\infty} \chi(n)f(n) + \mathcal{O}(f(x)).$$

En particular, se verifican las siguientes identidades:

$$\sum_{n\leq x} \frac{\chi(n)}{n} = \sum_{n=1}^{\infty} \frac{\chi(n)}{n} + \mathcal{O}\left(\frac{1}{x}\right), \qquad \sum_{n\leq x} \frac{\chi(n)\log n}{n} = \sum_{n=1}^{\infty} \frac{\chi(n)\log n}{n} + \mathcal{O}\left(\frac{\log x}{x}\right),$$

$$\sum_{n\leq x} \frac{\chi(n)}{\sqrt{n}} = \sum_{n=1}^{\infty} \frac{\chi(n)}{\sqrt{n}} + \mathcal{O}\left(\frac{1}{\sqrt{x}}\right).$$

Demostración. Sea χ un caracter no principal módulo q.

$$A(x) = \sum_{n\leq x} \chi(n).$$

Al ser χ no principal, por la Proposición 2.2, se tiene:

$$A(q) = \sum_{n=1}^{q} \chi(n) = 0,$$

y de la definición de χ se deduce que para todo k natural, $A(kq) = 0$. Por tanto $|A(x)| < |A(q)| = \varphi(q)$ y así, $A(x) = \mathcal{O}(1)$. Como por hipótesis $f(y) < f(x)$, empleando ahora (14) se verifica:

$$\sum_{x<n\leq y} \chi(n)f(n) = A(y)f(y) - A(x)f(x) - \int_x^y A(t)f'(t)\,dt = \mathcal{O}(f(y)) + \mathcal{O}(f(x)) + \mathcal{O}\left(\int_x^y f'(t)\,dt\right) = \mathcal{O}(f(x)).$$

Si además $\lim_{x\to\infty} f(x) = 0$, entonces para todo $\varepsilon > 0$ existe una constante $M > 0$ tal que para todo $x > M$ es $|f(x)| < \varepsilon$. Luego para $N_2 > N_1 > M$ se tiene aplicando lo que se acaba de probar:

$$\left|\sum_{N_1<n\leq N_2} \chi(n)f(n)\right| \leq C|f(N_1)| < C\varepsilon.$$

Aplicando el *criterio de convergencia de Cauchy*, la serie:

$$\sum_{n=1}^{\infty} \chi(n)f(n)$$

es convergente y se concluye:

$$\sum_{n=1}^{\infty}\chi(n)f(n)=\sum_{n\leq x}\chi(n)f(n)+\lim_{y\to\infty}\sum_{x<n\leq y}\chi(n)f(n)=\sum_{n\leq x}\chi(n)f(n)+\mathcal{O}(f(x)).$$

Finalmente, tomando respectivamente $f(x)=1/x$, $f(x)=\log(x)/x$ y $f(x)=1/\sqrt{x}$ para $x\geq 1$, se deducen de forma inmediata las tres identidades. □

De las tres identidades que han podido deducirse del resultado anterior, tomando las series infinitas que aparecen en las dos primeras, éstas serán las más importantes para el objetivo buscado:

Definición 2.4 *Sea χ un caracter de Dirichlet módulo q y $s\in\mathbb{C}$. Se define la función L de Dirichlet como la serie infinita:*

$$L(s,\chi)=\sum_{n=1}^{\infty}\frac{\chi(n)}{n^s}.$$

Como función de la variable compleja s, $L(s,\chi)$ se define para $\mathrm{Re}(s)>1$, donde la serie converge absolutamente. Además, admite una derivada respecto de s que corresponde a la serie infinita:

$$L'(s,\chi)=-\sum_{n=1}^{\infty}\frac{\chi(n)\log n}{n^s}.$$

En el límite de la región de convergencia absoluta, cuando $s\to 1^+$, se dan los valores especiales $L(1,\chi)$ y $L'(1,\chi)$, que gracias a la Proposición 2.3 definen series convergentes siempre que $\chi\neq\chi_0$, por lo que en ese caso quedan también bien definidos. De hecho, puede precisarse un poco más sobre ellos:

Proposicion 2.5 *(Propiedad de no anulación) $L(1,\chi)\neq 0$ para todo caracter χ real no principal.*

Demostración. Sea la función

$$X(n)=\sum_{d|n}\chi(d).$$

$X(n)$ es una función multiplicativa por (3) ya que χ es multiplicativa. Véase que para todo n se verifica que $X(n)\geq 0$ y si además n es un cuadrado, $X(n)\geq 1$. En efecto, para $n=p^k$ se tiene:

$$X(p^k)=\sum_{j=0}^{k}\chi(p^j)=1+\sum_{j=1}^{k}\chi^j(p).$$

Al ser χ real, únicamente toma los valores 0, ± 1, por lo que $X(p^k)$ toma los valores 0 (si $\chi(p)=-1$ y k es impar), 1 (si $\chi(p)=0$ o $\chi(p)=-1$ y k es par) o $k+1$ (si $\chi(p)=1$). De todo esto se deduce que $X(p^k)\geq 1$ si k es par. Sea ahora $n=p_1^{k_1}\cdots p_r^{k_r}$. Por multiplicatividad se tiene:

$$X(n)=\prod_{j=1}^{r}X(p_j^{k_j}).$$

Cada factor es no negativo, por lo que $X(n)\geq 0$. Por otra parte, si n es un cuadrado, k_j es par para todo j y se concluye que $X(n)\geq 1$. Una vez visto esto, sea ahora la función:

$$A(x)=\sum_{n\leq x}\frac{X(n)}{\sqrt{n}}.$$

La serie total asociada es divergente, ya que:

$$A(x)\geq\sum_{\substack{n\leq x\\ n=m^2}}\frac{1}{\sqrt{n}}=\sum_{m\leq\sqrt{x}}\frac{1}{m}\longrightarrow+\infty,\quad\text{cuando } x\to+\infty.$$

Véase ahora que $A(x)=2\sqrt{x}L(1,\chi)+\mathcal{O}(1)$ para todo $x\geq 1$. Para ello, se efectúa el siguiente desarrollo:

$$A(x)=\sum_{n\leq x}\frac{1}{\sqrt{n}}\sum_{d|n}\chi(d)=\sum_{dd'\leq x}\frac{\chi(d)}{\sqrt{dd'}}.$$

Aplicando (7) a la suma interior con $x_1 = x_2 = \sqrt{x}$, $f(n) = \chi(n)/\sqrt{n}$ y $g(n) = 1/\sqrt{n}$ se obtiene:

$$A(x) = \sum_{dd' \leq x} \frac{\chi(d)}{\sqrt{dd'}} = \sum_{n \leq \sqrt{x}} \frac{\chi(n)}{\sqrt{n}} G\left(\frac{x}{n}\right) + \sum_{n \leq \sqrt{x}} \frac{1}{\sqrt{n}} F\left(\frac{x}{n}\right) - F(\sqrt{x})G(\sqrt{x}),$$

donde, gracias a (24) y a la Proposición 2.3:

$$F(x) = \sum_{n \leq x} \frac{\chi(n)}{\sqrt{n}} = \sum_{n=1}^{\infty} \frac{\chi(n)}{\sqrt{n}} + \mathcal{O}\left(\frac{1}{\sqrt{x}}\right), \qquad G(x) = \sum_{n \leq x} \frac{1}{\sqrt{n}} = 2\sqrt{x} + C + \mathcal{O}\left(\frac{1}{\sqrt{x}}\right).$$

Sustituyendo ambas expresiones en la identidad anterior, denotando S a la serie infinita que aparece en $F(x)$ y volviendo a aplicar los resultados mencionados, se verifica:

$$\begin{aligned} A(x) = 2\sqrt{x} \sum_{n \leq \sqrt{x}} \frac{\chi(n)}{n} + C \sum_{n \leq \sqrt{x}} \frac{\chi(n)}{\sqrt{n}} + S \sum_{n \leq \sqrt{x}} \frac{1}{\sqrt{n}} - 2Sx^{\frac{1}{4}} + \mathcal{O}\left(\frac{1}{\sqrt{x}} \sum_{n \leq \sqrt{x}} |\chi(n)|\right) + \mathcal{O}\left(\frac{1}{\sqrt{x}} \sum_{n \leq \sqrt{x}} 1\right) + \mathcal{O}(1) \\ = 2\sqrt{x} \sum_{n=1}^{\infty} \frac{\chi(n)}{n} + \mathcal{O}(1) = 2\sqrt{x} L(1, \chi) + \mathcal{O}(1). \end{aligned}$$

Como $A(x) \longrightarrow +\infty$, se concluye que necesariamente $L(1, \chi) \neq 0$. □

La propiedad $L(1, \chi) \neq 0$ no es exclusiva de los caracteres reales y además se muestra de forma mucho más sencilla si χ es complejo. Si fuera $L(1, \chi) = 0$ para χ complejo, entonces $L(1, \overline{\chi}) = 0$ y el producto:

$$\prod_{\chi \,(\mathrm{mod}\, q)} L(s, \chi)$$

tendría un cero en $s = 1$, lo cual contradice el hecho de que el producto sea en realidad una serie de Dirichlet cuyo término general a_n/n^s verifica $a_n \geq 0$ y $a_1 = \prod \chi(1) = 1$. Esta propiedad de no anulación implica directamente que el cociente $L'(s, \chi)/L(s, \chi)$ no tiene un polo en $s = 1$ para $\chi \neq \chi_0$, lo cual será utilizado en la prueba de la infinitud de primos en progresiones aritméticas que se busca.

Respecto al caso $\chi = \chi_0$, nótese que la función $L(s, \chi_0)$ es similar a la función zeta de Riemann $\zeta(s)$:

Lema 2.6 *(Relación entre $\zeta(s)$ y $L(s, \chi_0)$) Se tiene:*

$$L(s, \chi_0) = \zeta(s) \prod_{p|q} (1 - p^{-s}).$$

Demostración. Como se muestra en (12), $\zeta(s)$ y $L(s, \chi_0)$ admiten sendos productos de Euler:

$$\zeta(s) = \prod_{p} \frac{1}{1 - p^{-s}}, \qquad L(s, \chi_0) = \prod_{p} \frac{1}{1 - \chi_0(p) p^{-s}}.$$

Comparando ambos productos, se obtiene la identidad buscada. En realidad se puede observar que la función $L(s, \chi_0)$ es similar a la función zeta de Riemann $\zeta(s)$ salvo por aquellos primos que dividen a q, los cuales no contribuyen a la suma. □

Sea el conjunto $A = \{1\} \cup \{p_1 \cdots p_r \,:\, p_i | q \text{ para todo } i,\, p_i \neq p_j \text{ para todo } i \neq j\}$. Entonces el producto finito que relaciona $\zeta(s)$ con $L(s, \chi_0)$ puede expresarse como:

$$\prod_{p|q} (1 - p^{-s}) = \sum_{n \in A} \frac{(-1)^{\omega(n)}}{n^s}.$$

Esta nueva forma del producto permitirá derivarlo con mayor facilidad. Además, para aprovechar convenientemente la relación entre $\zeta(s)$ y $L(s, \chi_0)$, se utilizará el siguiente resultado conocido:

Proposicion 2.7 *(Fórmula de Mertens) Se cumple para todo $x \geq 1$:*

$$\sum_{p \leq x} \frac{\log p}{p} = \log x + \mathcal{O}(1).$$

Demostración. Partiendo de la segunda identidad de (5) aplicada a la función $\Lambda(n)$ se tiene utilizando (11) y (20):

$$f(x) := \sum_{n\leq x} \Lambda(n) \left\lfloor \frac{x}{n} \right\rfloor = \sum_{n\leq x} \sum_{d|n} \Lambda(d) = \sum_{n\leq x} \log n = x \log x + \mathcal{O}(x).$$

Sea $t/2 < n \leq t$. Entonces $1 \leq t/n < 2$ y así $\lfloor t/n \rfloor = 1$. Esto permite deducir por (20):

$$\sum_{\frac{t}{2}<n\leq t} \Lambda(n) = \sum_{\frac{t}{2}<n\leq t} \Lambda(n) \left\lfloor \frac{t}{n} \right\rfloor \leq f(t) - 2f\left(\frac{t}{2}\right) = t \log t - 2 \cdot \frac{t}{2} \log \frac{t}{2} + \mathcal{O}(t) = \mathcal{O}(t).$$

En consecuencia:

$$\sum_{n\leq x} \Lambda(n) = \sum_{1\leq 2^m \leq x} \sum_{\frac{x}{2^{m+1}}<n\leq \frac{x}{2^m}} \Lambda(n) = \sum_{1\leq 2^m \leq x} \mathcal{O}\left(\frac{x}{2^m}\right) = \mathcal{O}\left(x \sum_{m=0}^{\infty} \frac{1}{2^m}\right) = \mathcal{O}(x).$$

De aquí se sigue que es posible eliminar la parte entera en $f(x)$ y como la parte fraccionaria siempre es $\mathcal{O}(1)$, se obtiene:

$$x \log x + \mathcal{O}(x) = \sum_{n\leq x} \Lambda(n) \left\lfloor \frac{x}{n} \right\rfloor = \sum_{n\leq x} \Lambda(n) \frac{x}{n} + \mathcal{O}\left(\sum_{n\leq x} \Lambda(n)\right) = x \sum_{n\leq x} \frac{\Lambda(n)}{n} + \mathcal{O}(x).$$

Por último, basta observar que por definición de $\Lambda(n)$, si α es el menor exponente tal que $p^{\alpha+1} > x$ para todo p, como $\log t = \mathcal{O}(t^{\varepsilon})$ para todo $\varepsilon > 0$, entonces:

$$\sum_{n\leq x} \frac{\Lambda(n)}{n} = \sum_{p\leq x} \frac{\log p}{p} + \sum_{k=2}^{\alpha} \sum_{p^k\leq x} \frac{\log p}{p^k} = \sum_{p\leq x} \frac{\log p}{p} + \mathcal{O}\left(\sum_{k=2}^{\alpha} \sum_{n=1}^{\infty} \frac{1}{n^{k-\varepsilon}}\right) = \sum_{p\leq x} \frac{\log p}{p} + \mathcal{O}(1).$$

Sustituyendo este resultado se concluye el enunciado. □

Al tomar límite cuando $x \to \infty$ en la *Fórmula de Mertens*, se obtiene:

$$\sum_{p} \frac{\log p}{p} = +\infty,$$

que refleja obviamente la infinitud de los primos. Este hecho implica que el cociente $\zeta'(s)/\zeta(s)$ tiene un polo en $s = 1$, ya que recurriendo a (8) para las series de Dirichlet de $\zeta'(s)$ y $1/\zeta(s)$ dadas por (10) y (9) respectivamente y bien definidas para $\mathrm{Re}(s) > 1$, se deduce por (11):

$$\lim_{s\to 1^+} \frac{\zeta'(s)}{\zeta(s)} = \lim_{s\to 1^+} \sum_{n=1}^{\infty} \frac{(\mu * \log)(n)}{n^s} = \sum_{n=1}^{\infty} \frac{\Lambda(n)}{n} = \sum_{p} \frac{\log p}{p} + \sum_{k=2}^{\infty} \sum_{p} \frac{\log p}{p^k} = +\infty.$$

Con esto se puede proceder a probar el resultado que responde a la segunda cuestión planteada en la Sección 1:

Teorema 2.8 *(Teorema de Dirichlet de primos en progresiones aritméticas) Existen infinitos primos en la progresión $a + nq$ con $n \geq 1$.*

Demostración. En primer lugar, gracias a la convolución $\mathbf{1} * \mu = id$ utilizada para probar (9) y a que los caracteres de Dirichlet son funciones completamente multiplicativas, se deduce que $\mathbf{1}\chi * \mu\chi = (\mathbf{1} * \mu)\chi = id \cdot \chi$. Por tanto, recurriendo a (8):

$$L(s,\chi) \sum_{n=1}^{\infty} \frac{\chi(n)\mu(n)}{n^s} = \sum_{n=1}^{\infty} \frac{\chi(n) id(n)}{n^s} = 1.$$

Por esto y por la definición de $L'(s,\chi)$, multiplicando ambas series y empleando (8) y (11) una vez más, se tiene para $\chi \neq \chi_0$:

$$-\frac{L'(s,\chi)}{L(s,\chi)} = \sum_{n=1}^{\infty} \frac{\chi(n)\Lambda(n)}{n^s}.$$

Por otra parte, recuperando la relación entre $\zeta(s)$ y $L(s,\chi_0)$ (Lema 2.6) se obtiene:

$$\frac{L'(s,\chi_0)}{L(s,\chi_0)} = \frac{\zeta'(s)\prod_{p|q}(1-p^{-s}) + \zeta(s)\sum_{n\in A}(-1)^{\omega(n)+1}\frac{\log n}{n^s}}{\zeta(s)\prod_{p|q}(1-p^{-s})} = \frac{\zeta'(s)}{\zeta(s)} + \mathcal{O}(1).$$

Usando ahora las *relaciones de ortogonalidad* de los caracteres de Dirichlet (Proposición 2.2.(B)) se deduce por las Proposiciones 2.5 y 2.7 y sus desarrollos posteriores:

$$\lim_{s\to 1^+} \varphi(q) \sum_{n\equiv a \,(\mathrm{mod}\, q)} \frac{\Lambda(n)}{n^s} = \lim_{s\to 1^+} \sum_{\chi \,(\mathrm{mod}\, q)} \sum_{n=1}^{\infty} \frac{\chi(n)\Lambda(n)}{n^s} \cdot \overline{\chi}(a)$$

$$= \lim_{s\to 1^+} \left(- \sum_{\chi\neq\chi_0} \frac{L'(s,\chi)}{L(s,\chi)} \cdot \overline{\chi}(a) - \frac{\zeta'(s)}{\zeta(s)} + \mathcal{O}(1) \right) = \mathcal{O}(1) + \infty.$$

Con esto se concluye el enunciado, ya que al ser $\log p/p \leq 1$ para todo primo p:

$$+\infty = \sum_{n\equiv a \,(\mathrm{mod}\, q)} \frac{\Lambda(n)}{n} = \sum_{p\equiv a \,(\mathrm{mod}\, q)} \frac{\log p}{p} + \sum_{k=2}^{\infty} \sum_{p^k\equiv a \,(\mathrm{mod}\, q)} \frac{\log p}{p^k}$$

$$= \sum_{p\equiv a \,(\mathrm{mod}\, q)} \frac{\log p}{p} + \mathcal{O}\left(\sum_{k=2}^{\infty} \sum_{n=1}^{\infty} \frac{1}{n^{k-\varepsilon}} \right) = \sum_{p\equiv a \,(\mathrm{mod}\, q)} \frac{\log p}{p} + \mathcal{O}(1),$$

de donde:

$$+\infty = \sum_{p\equiv a \,(\mathrm{mod}\, q)} \frac{\log p}{p} \leq \sum_{p\equiv a \,(\mathrm{mod}\, q)} 1 = \#\{p \equiv a \,(\mathrm{mod}\, q)\}.$$

□

§3. Extensión de la prueba de Iwaniec para el Teorema de los Números Primos en Progresiones Aritméticas

El objetivo que se persigue es intentar reproducir y extender la prueba que Iwaniec dedujo para el *Teorema de los Números Primos* al caso del *Teorema de los Números Primos en Progresiones Aritméticas*, y así dar respuesta a la última cuestión que se planteó al final de la Sección 1. Podría parecer que la extensión es inmediata, y de hecho en cierta forma es así, pero si establecemos la analogía en que en el caso de las progresiones aritméticas haya que utilizar las funciones L de Dirichlet $L(s,\chi)$ en lugar de $\zeta(s)$, existen varios detalles que cambian ciertas partes del argumento de Iwaniec, ya que el comportamiento de $L(s,\chi)$ cuando $\chi \neq \chi_0$ no es igual al de $\zeta(s)$ especialmente en el entorno del punto $s = 1$, hecho que es clave en la demostración de Iwaniec. Sin embargo, como se verá, esto no supone un obstáculo insalvable para poder reproducir el argumento de dicha demostración.

A. Enunciados equivalentes del Teorema de los Números Primos en Progresiones Aritméticas. Gracias al *Teorema de Dirichlet*, cobra sentido el estudiar un comportamiento asintótico para los primos que pertenecen a una cierta progresión aritmética. Análogamente a como sucedía en el caso del *Teorema de los Números Primos*, no existe una forma única de establecer un enunciado para el resultado y en la literatura se han originado pruebas tanto analíticas como elementales para varios de ellos. En esta sección se van a recordar las equivalencias entre los tres enunciados más clásicos del *Teorema de los Números Primos en Progresiones Aritméticas* para posteriormente proceder a demostrar el tercero de ellos siguiendo el argumento de Iwaniec para el caso sin progresiones aritméticas.

Teorema 2.9 *Los siguientes enunciados del Teorema de los Números Primos en Progresiones Aritméticas son equivalentes:*

(A) $\pi_{a,q}(x) := \sum_{\substack{p\leq x \\ p\equiv a \,(\mathrm{mod}\, q)}} 1 \sim \frac{x}{\varphi(q)\log x}.$

(B) $\psi_\chi(x) := \sum_{n\leq x} \chi(n)\Lambda(n) \sim \begin{cases} x & si\ \chi = \chi_0, \\ o(x) & si\ \chi \neq \chi_0. \end{cases}$

(C) $M_\chi(x) := \sum_{n\leq x} \chi(n)\mu(n) = o(x).$

Demostración $(A) \Leftrightarrow (B)$. Sea la función auxiliar:

$$\theta_\chi(x) := \sum_{p \le x} \chi(p) \log p.$$

Se tiene la siguiente relación entre $\psi_\chi(x)$ y $\theta_\chi(x)$:

$$\psi_\chi(x) = \sum_{m=1}^{\infty} \sum_{p^m \le x} \chi(p^m)\Lambda(p^m) = \sum_{m=1}^{\infty} \sum_{p \le x^{1/m}} \chi(p)^m \log p = \sum_{m \le \frac{\log x}{\log 2}} \sum_{p \le x^{1/m}} \chi(p)^m \log p = \sum_{m \le \frac{\log x}{\log 2}} \theta_{\chi^m}(x^{\frac{1}{m}}).$$

Tomando la diferencia entre ambas funciones se llega a:

$$0 \le |\psi_\chi(x) - \theta_\chi(x)| = \left| \sum_{2 \le m \le \frac{\log x}{\log 2}} x^{\frac{1}{m}} \log x^{\frac{1}{m}} \right| \le \sum_{2 \le m \le \frac{\log x}{\log 2}} x^{\frac{1}{m}} \log x^{\frac{1}{m}} \le \frac{\sqrt{x} \log^2 x}{2 \log 2}.$$

Dividiendo por x y tomando límite, se tiene:

$$\lim_{x \to +\infty} \left| \frac{\psi_\chi(x)}{x} - \frac{\theta_\chi(x)}{x} \right| = 0.$$

Esto quiere decir que $\psi_\chi(x)/x = \theta_\chi(x)/x + o(1)$, por lo que los límites de ambos cocientes, si existen, coinciden. Por otra parte, se busca ahora una relación entre $\theta_\chi(x)$ y $\pi_{a,q}(x)$. Si a no es coprimo con q se sabe que $\chi(a) = 0$. Por tanto:

$$\theta_\chi(x) = \sum_{p \le x} \chi(p) \log p = \sum_{\substack{a=1 \\ \mathrm{mcd}(a,q)=1}}^{q} \chi(a) \sum_{\substack{p \le x \\ p \equiv a \,(\mathrm{mod}\, q)}} \log p.$$

Sea $a_n = 1$ si $n = p \equiv a \,(\mathrm{mod}\, q)$ y $a_n = 0$ en otro caso. Aplicando (14) a la expresión de $\theta_\chi(x)$ y dividiendo por x se deduce:

$$\frac{\theta_\chi(x)}{x} = \frac{1}{x} \sum_{\substack{a=1 \\ \mathrm{mcd}(a,q)=1}}^{q} \chi(a) \sum_{n \le x} a_n \log n = \sum_{\substack{a=1 \\ \mathrm{mcd}(a,q)=1}}^{q} \chi(a) \left(\frac{\pi_{a,q}(x) \log x}{x} - \frac{\pi_{a,q}(2) \log 2}{x} - \frac{1}{x} \int_2^x \frac{\pi_{a,q}(t)}{t}\, dt \right).$$

Para analizar el término integral que aparece, se utiliza la hipótesis (A), por lo que $\pi_{a,q}(t)/t \sim 1/(\varphi(q) \log t)$. Esto de nuevo quiere decir que $\pi_{a,q}(t)/t = 1/(\varphi(q) \log t) + o(1/\log t) = \mathcal{O}(1/\log t)$. De esta manera, la expresión integral que quedaría dentro del término en $\mathcal{O}$ puede acotarse subdividiendo en los intervalos $[2, \sqrt{x}]$ y $[\sqrt{x}, x]$, obteniendo:

$$\frac{1}{x} \int_2^x \frac{dt}{\log t} \ll \frac{1}{\sqrt{x}} + \frac{x - \sqrt{x}}{x \log x}.$$

Al tomar límite cuando $x \to +\infty$ y aplicar (A) se concluye:

$$\lim_{x \to +\infty} \frac{\theta_\chi(x)}{x} = \sum_{\substack{a=1 \\ \mathrm{mcd}(a,q)=1}}^{q} \chi(a) \lim_{x \to +\infty} \frac{\pi_{a,q}(x) \log x}{x} = \frac{1}{\varphi(q)} \sum_{\substack{a=1 \\ \mathrm{mcd}(a,q)=1}}^{q} \chi(a) = \begin{cases} 1 & \text{si } \chi = \chi_0, \\ 0 & \text{si } \chi \neq \chi_0. \end{cases}$$

Con esto se tendría que $(A) \Rightarrow (B)$. Empleando de nuevo (14) para la expresión de $\pi_{a,q}(x)$ y dividiendo entre $x/\log x$ se deduce:

$$\begin{aligned} \frac{\pi_{a,q}(x) \log x}{x} &= \frac{\log x}{x} \sum_{1 < n \le x} a_n \log n \cdot \frac{1}{\log n} \\ &= \frac{\log x}{x} \left(\sum_{1 < n \le x} a_n \log n - a_2 \log 2 \right) + \frac{\log x}{x} \int_2^x \left(\sum_{1 < n \le t} a_n \log n \right) \frac{dt}{t \log^2 t}, \end{aligned}$$

donde gracias a las *relaciones de ortogonalidad* de los caracteres de Dirichlet (Proposición 2.2.(B)), se verifica:

$$\sum_{1 < n \le x} a_n \log n = \sum_{\substack{p \le x \\ p \equiv a \,(\mathrm{mod}\, q)}} \log p = \frac{1}{\varphi(q)} \sum_{\chi \bmod q} \overline{\chi}(a) \sum_{p \le x} \chi(p) \log p = \frac{1}{\varphi(q)} \sum_{\chi \bmod q} \overline{\chi}(a) \theta_\chi(x).$$

Sustituyendo esta expresión se llega a:

$$\frac{\pi_{a,q}(x)\log x}{x} = \frac{1}{\varphi(q)x}\sum_{\chi \bmod q}\overline{\chi}(a)\theta_\chi(x) + \frac{\log x}{x}\left(-a_2\log 2 + \frac{1}{\varphi(q)}\int_2^x\left(\sum_{\chi \bmod q}\overline{\chi}(a)\theta_\chi(t)\right)\frac{dt}{t\log^2 t}\right).$$

Por la hipótesis (B), se puede deducir que para cualquier χ, siempre $\theta_\chi(x) = \mathcal{O}(x)$. Aplicando esto, el término integral del miembro derecho puede acotarse subdividiendo una vez más en los intervalos $[2,\sqrt{x}]$ y $[\sqrt{x},x]$, obteniendo:

$$\frac{\log x}{x}\int_2^x \frac{dt}{\log^2 t} \ll \frac{\log x}{\sqrt{x}} + \frac{x-\sqrt{x}}{x\log x}.$$

Al tomar límite cuando $x \to +\infty$ y aplicar (B) se concluye:

$$\lim_{x\to+\infty}\frac{\pi_{a,q}(x)\log x}{x} = \frac{1}{\varphi(q)}\sum_{\chi \bmod q}\overline{\chi}(a)\lim_{x\to+\infty}\frac{\theta_\chi(x)}{x} = \frac{\overline{\chi_0}(a)}{\varphi(q)} = \frac{1}{\varphi(q)}.$$

□

Demostración $(A) \Rightarrow (C)$. Como punto de partida, por (5) y (11) se tiene:

$$\sum_{n\le x}\chi(n)\mu(n)\psi_\chi\left(\frac{x}{n}\right) = \sum_{n\le x}\chi(n)\mu(n)\sum_{m\le\frac{x}{n}}\chi(m)\Lambda(m) = \sum_{n\le x}\sum_{d|n}\chi(d)\mu(d)\chi\left(\frac{x}{d}\right)\Lambda\left(\frac{n}{d}\right)$$
$$= \sum_{n\le x}\chi(n)(\mu*\Lambda)(n) = -\sum_{n\le x}\chi(n)\mu(n)\log n.$$

Gracias a la equivalencia entre (A) y (B) se cumple:

$$\sum_{n\le x}\chi(n)\mu(n)\left(\psi_\chi\left(\frac{x}{n}\right) - \delta_\chi\left\lfloor\frac{x}{n}\right\rfloor\right) = \sum_{n\le x} o\left(\frac{x}{n}\right), \qquad \delta_\chi = \begin{cases}1 & \text{si } \chi = \chi_0,\\ 0 & \text{si } \chi \ne \chi_0.\end{cases}$$

En general, para una función $g:[1,\infty)\longrightarrow\mathbb{R}$ tal que $g(y) = o(y)$, dado $\varepsilon > 0$ existe cierto $T > 0$ tal que si $y > T$ entonces $|g(y)| < \varepsilon y$. En consecuencia:

$$\sum_{n\le x}\left|g\left(\frac{x}{n}\right)\right| = \sum_{n\le\frac{x}{N}}\left|g\left(\frac{x}{n}\right)\right| + \sum_{\frac{x}{T}<n\le x}\left|g\left(\frac{x}{n}\right)\right| \le \varepsilon x\sum_{n\le\frac{x}{T}}\frac{1}{n} + \sup_{j<T}|g(j)|\cdot x\left(1-\frac{1}{T}\right).$$

Aplicando (21) y dividendo entre $x\log x$, se deduce tomando límite superior:

$$\limsup_{x\to+\infty}\frac{1}{x\log x}\sum_{n\le x}\left|g\left(\frac{x}{n}\right)\right| \le \limsup_{x\to+\infty}\left(\varepsilon + \mathcal{O}\left(\frac{1}{\log x}\right)\right) = \varepsilon.$$

y para $\varepsilon \to 0$ se obtiene:

$$\sum_{n\le x}\left|g\left(\frac{x}{n}\right)\right| = o(x\log x).$$

Por otra parte, por definición de $\mu(n)$:

$$\sum_{d|p^k}\chi(d)\mu(d) = \sum_{j=0}^{k}\chi(p^j)\mu(p^j) = 1-\chi(p),$$

y utilizando (5) para $f = \chi\mu$, se cumple para $n = p_1^{k_1}\cdots p_r^{k_r}$ por multiplicatividad:

$$\sum_{n\le x}\chi(n)\mu(n)\left\lfloor\frac{x}{n}\right\rfloor = \sum_{n\le x}\sum_{d|n}\chi(d)\mu(d) = \sum_{n\le x}\prod_{j=1}^{r}(1-\chi(p_j)).$$

Teniendo en cuenta todo lo anterior, para $g(y) = \psi_\chi(y) - \delta_\chi y$ se deduce:

$$\left|\sum_{n\leq x}\chi(n)\mu(n)\log n\right| \leq \left|\sum_{n\leq x}\chi(n)\mu(n)g\left(\frac{x}{n}\right)\right| + \left|\sum_{n\leq x}\chi(n)\mu(n)\delta_\chi\left\lfloor\frac{x}{n}\right\rfloor\right|$$

$$\leq \sum_{n\leq x}\left|g\left(\frac{x}{n}\right)\right| + \left|\sum_{\substack{n\leq x\\ n=p_1^{k_1}\cdots p_r^{k_r}}}\prod_{j=1}^{r}(1-\chi_0(p_j))\right| \leq o(x\log x) + \lfloor x\rfloor.$$

Con esto se puede concluir:

$$\sum_{n\leq x}\chi(n)\mu(n)\log n = o(x\log x).$$

Si se emplea por último (14), el resultado es:

$$\sum_{n\leq x}\chi(n)\mu(n) = \sum_{n\leq x}\chi(n)\mu(n)\cdot\frac{\log n}{\log n} = \frac{o(x\log x)}{\log x} - \int_2^x o(t\log t)\frac{dt}{t\log^2 t} + \mathcal{O}(1) = o(x) + \int_2^x o\left(\frac{1}{\log t}\right)\,dt + \mathcal{O}(1).$$

El término integral que queda se trata de la siguiente forma: si $f(t) = o(1/\log t)$, entonces $f(t)\log t \longrightarrow 0$ cuando $t \to +\infty$. Se separa la integral como en otras ocasiones en dos partes según los intervalos $[2, \sqrt{x}]$ y $[\sqrt{x}, x]$. En el primero basta utilizar que $o(1/\log t) = o(1) = \mathcal{O}(1)$, por lo que al acotar de esta forma, la primera integral es $\mathcal{O}(\sqrt{x})$. En el segundo intervalo, si $f(t) = o(1/\log t)$, esto significa que $|f(t)| \leq \varepsilon(t)/\log t$, con $\varepsilon(t)$ tan pequeño como se quiera cuando $x \gg 0$, ya que en caso contrario no se cumpliría que $f(t)\log t \longrightarrow 0$. Por tanto, la segunda integral es $\mathcal{O}(\varepsilon x/\log x)$. Al unir ambas integrales y dividir entre $x/\log x$, se obtiene cuando $x \to +\infty$:

$$\frac{\log x}{x}\int_2^x o\left(\frac{1}{\log t}\right)\,dt \ll \frac{\log x}{\sqrt{x}} + \varepsilon \longrightarrow 0.$$

Con esto se puede deducir:

$$\int_2^x o\left(\frac{1}{\log t}\right)\,dt = o\left(\frac{x}{\log x}\right).$$

Sustituyendo esta última estimación y dividiendo entre x, se concluye:

$$\frac{1}{x}\sum_{n\leq x}\chi(n)\mu(n) = o(1) + o\left(\frac{1}{\log x}\right) + \mathcal{O}\left(\frac{1}{x}\right) = o(1).$$

□

Demostración $(C) \Rightarrow (A)$. Sea $\chi \neq \chi_0$. Para comenzar, se recurre a (5) y (11) para deducir:

$$\sum_{n\leq x}\chi(n)\Lambda(n) = \sum_{n\leq x}\chi(n)\sum_{d|n}\log d\mu\left(\frac{n}{d}\right) = \sum_{n\leq x}\sum_{d|n}\chi\left(\frac{n}{d}\right)\mu\left(\frac{n}{d}\right)\chi(d)\log d$$

$$= \sum_{n\leq x}\sum_{m\leq\frac{x}{n}}\chi(m)\mu(m)\chi(n)\log n = \sum_{n\leq x}\chi(n)\log n\sum_{d\leq\frac{x}{n}}\chi(d)\mu(d)$$

$$= \sum_{n\leq N}\chi(n)\log n\sum_{d\leq\frac{x}{n}}\chi(d)\mu(d) + \sum_{N<n\leq x}\chi(n)\log n\sum_{d\leq\frac{x}{n}}\chi(d)\mu(d).$$

Para la primera suma, se recurre a la hipótesis (C):

$$\sum_{d\leq t}\chi(d)\mu(d) = o(t)$$

para $t = x/n$ implica que para $t \geq T$ se cumple:

$$\left|\sum_{d\leq t}\chi(d)\mu(d)\right| < \varepsilon t.$$

Puesto que N es un número fijo, para $x \geq TN$ se tiene $x/n \geq x/N \geq T$, por lo que es posible aplicar la hipótesis y por la Proposición 2.3 se llega a:

$$\left| \sum_{n \leq N} \chi(n) \log n \sum_{d \leq \frac{x}{n}} \chi(d)\mu(d) \right| < \varepsilon x \left| \sum_{n \leq N} \frac{\chi(n) \log n}{n} \right| = \varepsilon x \left| \sum_{n=1}^{\infty} \frac{\chi(n) \log n}{n} + \mathcal{O}\left(\frac{\log N}{N} \right) \right|.$$

Esto quiere decir que la primera suma es $o(x)$. Para la segunda suma, se intercambia el orden de sumación y se utiliza (14) teniendo en cuenta que para $\chi \neq \chi_0$, se tiene:

$$\sum_{N < n \leq \frac{x}{d}} \chi(n) = \mathcal{O}(1).$$

De esta manera recurriendo además a la sumación de términos $\mathcal{O}$ en (19) y la división en intervalos diádicos se obtiene:

$$\begin{aligned} \sum_{N < n \leq x} \chi(n) \log n \sum_{d \leq \frac{x}{n}} \chi(d)\mu(d) &= \sum_{d \leq \frac{x}{N}} \chi(d)\mu(d) \sum_{N < n \leq \frac{x}{d}} \chi(n) \log n \\ &= \sum_{d \leq \frac{x}{N}} \chi(d)\mu(d) \left(\mathcal{O}(1) \left(\log \frac{x}{d} - \log N \right) - \int_N^{\frac{x}{d}} \mathcal{O}(1) \frac{dt}{t} \right) = \sum_{d \leq \frac{x}{N}} \mathcal{O}\left(\log \frac{x}{dN} \right) \\ &= \mathcal{O}\left(\sum_{1 \leq 2^n \leq \frac{x}{N}} \sum_{\frac{x}{2^{n+1}N} < d \leq \frac{x}{2^n N}} \log \frac{x}{dN} \right) = \mathcal{O}\left(\frac{x}{N} \sum_{m=1}^{\infty} \frac{m}{2^m} \right) = \mathcal{O}\left(\frac{x}{N} \right). \end{aligned}$$

Uniendo las estimaciones, el resultado es:

$$\psi_\chi(x) = o(x) + \mathcal{O}\left(\frac{x}{N} \right).$$

Al tomar límite superior y $N \to +\infty$, se concluye:

$$\limsup_{x \to +\infty} \left| \frac{\psi_\chi(x)}{x} \right| = \mathcal{O}\left(\frac{1}{N} \right) \longrightarrow 0.$$

Con esto[1]se ha probado (B), que es equivalente a (A) como se vio anteriormente. Para continuar, se analiza ahora el caso $\chi = \chi_0$, tomando como referencia las equivalencias existentes en los enunciados análogos para el *Teorema de los Números Primos*. Si $q = p$ primo, por la multiplicatividad de $\mu(n)$ se cumple:

$$\sum_{n \leq x} \mu(n) = \sum_{\substack{n \leq x \\ p \nmid n}} \mu(n) + \mu(p) \sum_{\substack{n \leq \frac{x}{p} \\ p \nmid n}} \mu(n) = \sum_{n \leq x} \chi_0(n)\mu(n) + \mu(p) \sum_{n \leq \frac{x}{p}} \chi_0(n)\mu(n),$$

donde el caracter χ_0 se toma módulo p. Por (C), ambas sumas interiores son $o(x)$, por lo que:

$$\sum_{n \leq x} \mu(n) = o(x).$$

Tomando ahora $q = p_1^{a_1} \cdots p_r^{a_r}$, de nuevo por la multiplicatividad de $\mu(n)$ el desarrollo anterior se cumple para cada primo p_j. Sumando las r identidades correspondientes a p_j se deduce:

$$\sum_{n \leq x} \mu(n) = \frac{1}{\omega(q)} \sum_{j=1}^{r} \left(\sum_{n \leq x} \chi_{0,j}(n)\mu(n) + \mu(p_j) \sum_{n \leq \frac{x}{p_j}} \chi_{0,j}(n)\mu(n) \right).$$

Aplicado a cada primo p_j, todas las sumas interiores son $o(x)$, por lo que:

$$\sum_{n \leq x} \mu(n) = o(x).$$

[1]Aunque no se ha especificado, en la asintótica $\psi_\chi(x) = o(x)$ para $\chi \neq \chi_0$ se sabe que el término de error depende de q pero de una forma que de momento es desconocida, algo que tiene que ver con ciertos valores especiales de las funciones L llamados *ceros de Siegel* [**?**], cuya existencia no se ha probado ni refutado.

Este enunciado es equivalente al *Teorema de los Números Primos*, que como se ha dicho se supone conocido. Esto implica en particular que $\psi(x) \sim x$ y de aquí faltaría deducir que $\psi_{\chi_0}(x) \sim x$. Para probarlo se procede así:

$$\psi_{\chi_0}(x) = \psi(x) - \sum_{\substack{n \leq x \\ \text{mcd}(n,q)>1}} \Lambda(n).$$

Bastaría ver que el termino restante es $o(x)$. La función $\Lambda(n)$ se anula en todos los enteros salvo en los casos $n = p^\alpha$ para $\alpha \geq 1$. Por tanto, si $\text{mcd}(p^\alpha, q) > 1$ y $q = p_1^{a_1} \cdots p_r^{a_r}$, entonces $p^\alpha = p_j^\alpha$ para algún $1 \leq j \leq r$. De aquí se deduce:

$$\sum_{\substack{n \leq x \\ \text{mcd}(n,q)>1}} \Lambda(n) = \sum_{\substack{p^\alpha \leq x \\ \text{mcd}(p^\alpha,q)>1}} \log p = \sum_{j=1}^{r} \sum_{p_j^\alpha \leq x} \log p_j = \sum_{j=1}^{r} \log p_j \sum_{\alpha \leq \frac{\log x}{\log p_j}} 1 \leq \sum_{j=1}^{r} \log p_j \cdot \frac{\log x}{\log p_j} = \omega(q) \log x.$$

Dividiendo entre x y tomando límite se concluye:

$$\lim_{x \to +\infty} \frac{1}{x} \sum_{\substack{n \leq x \\ \text{mcd}(n,q)>1}} \Lambda(n) = 0.$$

Esto implica que $\psi_{\chi_0}(x) \sim x$, y por la equivalencia entre (B) y (A) previamente probada, se tiene la implicación buscada. □

B. Integración compleja - Fórmula de Faà di Bruno. Antes de entrar en la extensión de la prueba de Iwaniec propiamente dicha, se presentan a continuación los resultados técnicos previos fundamentales que se aplicarán en la misma. El primero de ellos es una aplicación de la conocida *Fórmula Integral de Cauchy* de la teoría de *Variable Compleja*:

Proposicion 2.10 *Sea la función:*

$$(\log y)_+ = \begin{cases} \log y & si \ \ y > 1, \\ 0 & si \ \ 0 < y \leq 1. \end{cases}$$

Si $s = \sigma + it \in \mathbb{C}$, para $\sigma > 0$ e $y > 0$ se tiene:

$$(\log y)_+ = \frac{1}{2\pi i} \int_{\text{Re}(s)=\sigma} \frac{y^s}{s^2}\, ds.$$

Demostración. En primer lugar, sea $y > 1$. Dado $R > 0$ se toma $\Gamma = \gamma_1 \cup \gamma_2 \cup \gamma_3 \cup \gamma_4$ la región del plano complejo cuya frontera (recorrida en el sentido contrario al de las agujas del reloj) está delimitada por los caminos:

$$\gamma_1 = \{\sigma + it \,|\, t \in [-R, R]\}, \quad \gamma_2 = \{-\tau + iR \,|\, \tau \in [-\sigma, R]\},$$

$$\gamma_3 = \{-R - it \,|\, t \in [-R, R]\}, \quad \gamma_4 = \{\tau + iR \,|\, \tau \in [-R, \sigma]\}.$$

La *Fórmula Integral de Cauchy* sostiene que si $f(z)$ es holomorfa en una región Ω que incluye a una región Γ delimitada por un camino cerrado, entonces para todo $a \in \Gamma$ se tiene:

$$\frac{d^n f}{dz^n}(a) = \frac{n!}{2\pi i} \oint_\Gamma \frac{f(z)}{(z-a)^{n+1}}\, dz.$$

Por tanto, tomando $z = s$, $f(s) = y^s$, $a = 0$ y $n = 1$, se obtiene:

$$\oint_\Gamma \frac{y^s}{s^2}\, ds = 2\pi i \log y.$$

Si se subdivide la integral circular en la suma de las integrales de los caminos que conforman Γ, se pueden estimar tres de ellas directamente por definición de los γ_j de la siguiente forma:

$$\left| \int_{\gamma_j} \frac{y^s}{s^2}\, ds \right| \leq \text{long}(\gamma_j) \cdot \max_{\gamma_j} \left| \frac{y^s}{s^2} \right| = \text{long}(\gamma_j) \cdot \max \frac{y^{\text{Re}(\gamma_j(s))}}{\text{Re}(\gamma_j(s))^2 + \text{Im}(\gamma_j(s))^2} \overset{R \to \infty}{\longrightarrow} 0.$$

Tomando ahora $y = 1$, entonces $\log 1 = 0$ y se tiene:

$$\frac{1}{2\pi i}\int_{\mathrm{Re}(s)=\sigma}\frac{ds}{s^2} = \frac{1}{2\pi i}\int_{-\infty}^{+\infty}\frac{idt}{(\sigma+it)^2} = \frac{1}{2\pi i}\lim_{R\to\infty}\int_{-R}^{R}\frac{idt}{(\sigma+it)^2} = \frac{1}{\pi}\lim_{R\to\infty}\frac{R}{\sigma^2+R^2} = 0.$$

Para finalizar, sea $0 < y < 1$. Dado de nuevo $R > 0$ se toma $\Gamma' = \gamma_1 \cup \gamma_2' \cup \gamma_3' \cup \gamma_4'$ la región del plano complejo cuya frontera (recorrida en el sentido de las agujas del reloj) está delimitada por γ_1 y los caminos siguientes:

$$\gamma_2' = \{\tau + iR \,|\, \tau \in [\sigma, \sigma+R]\}, \quad \gamma_3' = \{\sigma + R - it \,|\, t \in [-R, R]\}, \quad \gamma_4' = \{-\tau - iR \,|\, \tau \in [-\sigma-R, -\sigma]\}.$$

En este caso, la función $f(s) = y^s s^{-2}$ es holomorfa en toda la región Γ', por lo que por el Teorema de Cauchy:

$$\frac{1}{2\pi i}\oint_{\Gamma'}\frac{y^s}{s^2}\,ds = 0.$$

Subdividiendo de nuevo la integral circular en la suma de las integrales de los caminos que conforman Γ', se vuelven a estimar tres de ellas de la misma forma:

$$\left|\int_{\gamma_j'}\frac{y^s}{s^2}\,ds\right| \le \mathrm{long}(\gamma_j')\cdot \max_{\gamma_j'}\left|\frac{y^s}{s^2}\right| = \mathrm{long}(\gamma_j')\cdot \max \frac{y^{\mathrm{Re}(\gamma_j'(s))}}{\mathrm{Re}(\gamma_j'(s))^2 + \mathrm{Im}(\gamma_j'(s))^2} \overset{R\to\infty}{\longrightarrow} 0.$$

Reuniendo todos los resultados en los tres casos se obtiene:

$$\int_{\gamma_1}\frac{y^s}{s^2}\,ds = (\log y)_+.$$

Por otra parte, se verifica la siguiente acotación por una función integrable:

$$\left|\frac{iy^{\sigma+it}}{(\sigma+it)^2}\chi_{[-R,R]}(t)\right| \le \frac{y^\sigma}{\sigma^2+t^2},$$

luego por el *Teorema de la Convergencia Dominada* el límite y la integral pueden intercambiarse y se concluye:

$$(\log y)_+ = \lim_{R\to\infty}\int_{\gamma_1}\frac{y^s}{s^2}\,ds = \lim_{R\to\infty}\int_{\mathbb{R}}\frac{iy^{\sigma+it}}{(\sigma+it)^2}\chi_{[-R,R]}(t)\,dt = i\int_{-\infty}^{+\infty}\frac{y^{\sigma+it}}{(\sigma+it)^2}\,dt = \int_{\mathrm{Re}(s)=\sigma}\frac{y^s}{s^2}\,ds.$$

□

El segundo resultado que se va a presentar es una versión de una fórmula del cálculo diferencial conocida como *Fórmula de Faà di Bruno* que expresa en su forma más general la derivada n-ésima de una composición de funciones en función de las derivadas de orden inferior. Para poder llegar a ella, se introduce en primer lugar una fórmula auxiliar:

Proposicion 2.11 *(Identidad multinomial) Si $y_1, \ldots, y_m$ son elementos conmutativos de un anillo ($y_i y_j = y_j y_i$ para cualesquiera $1 \le i < j \le m$), entonces para todo $n \ge 0$ se cumple:*

$$(y_1 + \ldots + y_m)^n = \sum_{a_1+\ldots+a_m=n}\frac{n!}{a_1!\cdots a_m!}y_1^{a_1}\cdots y_m^{a_m}.$$

Demostración. Se verifica directamente a través del *desarrollo de Taylor* en el punto $(0, \ldots, 0)$ de la función $(y_1 + \ldots + y_m)^n$. □

A partir de aquí es posible deducir el resultado buscado [**?**]:

Proposicion 2.12 *Se tiene:*

(*A*) *(Fórmula de Faà di Bruno) Si f y g son derivables hasta el orden $n \ge 1$ u holomorfas, entonces:*

$$(f\circ g)^{(n)}(x) = \sum_{j=1}^{n}\sum_{\substack{a_1+\ldots+a_n=j\\ a_1+2a_2+\ldots+na_n=n}}\frac{n!}{a_1!\cdots a_n!}\left(f^{(j)}\circ g\right)(x)\prod_{k=1}^{n}\left(\frac{g^{(k)}(x)}{k!}\right)^{a_k}.$$

(*B*) *En particular,*

$$\left(\frac{1}{g}\right)^{(n)}(x)=\frac{1}{g(x)}\sum_{a_1+\ldots+na_n=n}\frac{(-1)^{(a_1+\ldots+a_n)}n!(a_1+\ldots+a_n)!}{a_1!1!^{a_1}\cdots a_n!n!^{a_n}}\prod_{j=1}^{n}\left(\frac{g^{(j)}(x)}{g(x)}\right)^{a_j}.$$

Demostración.

(*A*) Se parte de la identidad:

$$(f\circ g)^{(n)}=\sum_{j=0}^{n}\left(f^{(j)}\circ g\right)\cdot P_{n,j}\left(g',\ldots,g^{(n)}\right),$$

donde los $P_{n,j}$ corresponden a ciertos polinomios definidos por recurrencia. Para comprobarla, es claro que $(f\circ g)^{(0)}=(f\circ g)\cdot P_{0,0}$ siendo $P_{0,0}=1$. Por tanto, suponiendo la identidad cierta hasta el orden $n-1$ de derivación, se concluye procediendo por inducción:

$$\begin{aligned}(f\circ g)^{(n)}&=\left((f\circ g)^{(n-1)}\right)'=\left(\sum_{j=0}^{n-1}\left(f^{(j)}\circ g\right)\cdot P_{n-1,j}\left(g',\ldots,g^{(n-1)}\right)\right)'\\&=\sum_{j=0}^{n}\left(\left(f^{(j+1)}\circ g\right)\cdot g'\cdot P_{n-1,j}\left(g',\ldots,g^{(n-1)}\right)+\left(f^{(j)}\cdot g\right)\cdot\sum_{k=1}^{n-1}g^{(k+1)}\cdot\frac{\partial P_{n-1,j}\left(g',\ldots,g^{(n-1)}\right)}{\partial g^{(k)}}\right)\\&=\sum_{j=0}^{n}\left(f^{(j)}\circ g\right)\cdot P_{n,j}\left(g',\ldots,g^{(n)}\right),\end{aligned}$$

donde:

$$P_{n,j}\left(g',\ldots,g^{(n)}\right):=g'\cdot P_{n-1,j-1}\left(g',\ldots,g^{(n-1)}\right)+\sum_{k=1}^{n-1}g^{(k+1)}\cdot\frac{\partial P_{n-1,j}\left(g',\ldots,g^{(n-1)}\right)}{\partial g^{(k)}},$$

$$0\leq j\leq n,\qquad P_{n-1,-1}=0=P_{n-1,n}.$$

Como consecuencia de esta identidad, se puede observar que si se aplica a un punto x_0 particular, $(f\circ g)^{(n)}(x_0)$ solo depende los valores $g^{(j)}(x_0)$ y $f^{(j)}(g(x_0))$ para todo j. Por tanto, la validez de (A) se tendría no solo para f y g, sino para cualesquiera funciones F y G que en x_0 tengan las mismas derivadas hasta el orden n que f y g. Esto permite suponer sin pérdida de generalidad que f y g son polinomios (de hecho, F y G pueden ser aproximadas por sus respectivos polinomios de Taylor de grado n). Por otra parte, ya que las traslaciones $x-x_0$ y $g(x)-g(x_0)$ no alteran la expresión de (A), es posible suponer de nuevo sin pérdida de generalidad que $x_0=0$ y $g(x_0)=0$. Así se puede escribir $f(x)=f_0+f_1x+\ldots+f_nx^n$ y $g(x)=g_1x+\ldots+g_nx^n$, donde $f_j=f^{(j)}(0)/j!$ y $g_j=g^{(j)}(0)/j!$ para todo j. Aplicando directamente la *Identidad Multinomial* (Proposición 2.11) para $y_k:=g_kx^k$ se llega a:

$$(f\circ g)(x)=\sum_{j=0}^{n}f_j(g_1x+\ldots+g_nx^n)^j=\sum_{j=0}^{n}f_j\sum_{a_1+\ldots+a_n=j}\frac{j!}{a_1!\cdots a_n!}g_1^{a_1}\cdots g_n^{a_n}x^{a_1+2a_2+\ldots+na_n}.$$

Dado n se tendrá en algún momento $a_1+2a_2+\ldots+na_n=n$ y el coeficiente de x^n en $(f\circ g)(x)$ vendría dado entonces por:

$$(f\circ g)^{(n)}(0)/n!=\sum_{j=0}^{n}f_j\sum_{\substack{a_1+\ldots+a_n=j\\a_1+2a_2+\ldots+na_n=n}}\frac{j!}{a_1!\cdots a_n!}g_1^{a_1}\cdots g_n^{a_n}.$$

Esta identidad demuestra que se tiene (A) en $x_0=0$ y por consiguiente se cumple para todo x.

(*B*) Basta aplicar directamente lo anterior al caso en que $f(x)=1/x$, teniendo en cuenta que $f^{(j)}(x)=(-1)^jj!/x^{j+1}$. De esta forma:

$$\left(\frac{1}{g}\right)^{(n)}(x)=\frac{n!}{g(x)}\sum_{j=0}^{n}(-1)^jj!\sum_{\substack{a_1+\ldots+a_n=j\\a_1+\ldots+na_n=n}}\frac{1}{a_1!1!^{a_1}\cdots a_n!n!^{a_n}}\prod_{j=1}^{n}\left(\frac{g^{(j)}(x)}{g(x)}\right)^{a_j},$$

que es equivalente al enunciado. □

C. Cotas para $L(s,\chi)$ y sus derivadas. Aparte de los aspectos mencionados en el apartado anterior, en la prueba de Iwaniec es importante y delicada la utilización del comportamiento de la función $\zeta(s)$ cerca de $s=1$ en beneficio propio, probando las siguientes estimaciones [?] para $k\geq 0$ y σ cerca de 1:

$$(-1)^k\zeta^{(k)}(s)=\frac{k!}{(s-1)^{k+1}}+\mathcal{O}_k\left(\log^{k+1}(2|s|)\right)\quad\Rightarrow\quad(\zeta^*)^{(k)}(s)=\mathcal{O}_k\left(|s|\log^{k+1}(2|s|)\right),\tag{2.1}$$

$$|\zeta^*(s)|\gg(\sigma-1)^{\frac{3}{4}}|s|\log^{-\frac{1}{4}}(2|s|),\tag{2.2}$$

donde $\zeta^*(s):=(s-1)\zeta(s)$. Estableciendo una analogía para las funciones L de Dirichlet, hay que tener en cuenta que aunque no se especificará explícitamente para no complicar la notación, las constantes en todas las acotaciones dependerán de q, lo cual puede intuirse siguiendo el argumento de cada demostración de este apartado. Asimismo, ya que lo interesante es trabajar cerca de $s=1$, se tomará $1<\sigma<2$, lo que será suficiente para todo lo que se busca. Antes de probar las acotaciones se presenta un pequeño resultado auxiliar:

Lema 2.13 *Para todo $k\geq 0$, $x>2$ y $s=\sigma+i\tau$ con $1<\sigma<2$ se verifican:*

$$\int_x^\infty\frac{\log^k t}{t^{\sigma+1}}\,dt\ll_k\frac{\log^k x}{x}.$$

Demostración. Se emplea directamente la *regla de L'Hôpital*:

$$\lim_{x\to\infty}\frac{\int_x^\infty\log^k t\cdot t^{-\sigma-1}\,dt}{\log^k x\cdot x^{-\sigma}}=\lim_{x\to\infty}\frac{-1}{\frac{k}{\log x}-\sigma}=\frac{1}{\sigma}<\infty,$$

ya que $1<\sigma<2$. Por tanto, existe una constante (no dependiente de σ) tal que la desigualdad es válida. □

Con este resultado es posible comenzar a probar las acotaciones que se necesitan, reescribiendo en parte el procedimiento de Iwaniec para $\zeta(s)$ aplicado a las funciones $L(s,\chi)$:

Proposicion 2.14 *(Cotas superiores para $L^{(k)}(s,\chi)$) Sea $1<\sigma<2$.*

(A) *Para $\chi=\chi_0$, sea $L^*(s,\chi_0):=(s-1)L(s,\chi_0)$. Entonces:*

$$(L^*)^{(k)}(s,\chi_0)=\mathcal{O}_k\left(|s|\log^{k+1}(2|s|)\right).$$

(B) *Para $\chi\neq\chi_0$:*

$$L^{(k)}(s,\chi)=\mathcal{O}_k\left(\log^{k+1}(2|s|)\right).$$

Demostración.

(A) Recuperando la identidad vista tras la prueba del Lema 2.6:

$$\prod_{p|q}(1-p^{-s})=\sum_{n\in A}\frac{(-1)^{\omega(n)}}{n^s},$$

se deduce al aplicar el Lema 2.6 y la *Regla de Leibniz* para la derivada k-ésima del producto de dos funciones:

$$\begin{aligned}(L^*)^{(k)}(s,\chi_0)=\left(\zeta^*(s)\prod_{p|q}(1-p^{-s})\right)^{(k)}&=\sum_{j=0}^k\binom{k}{j}(\zeta^*)^{(j)}(s)\left(\prod_{p|q}(1-p^{-s})\right)^{(k-j)}\\&=\sum_{j=0}^k\binom{k}{j}(\zeta^*)^{(j)}(s)\left(\sum_{n\in A}(-1)^{k-j+\omega(n)}\frac{\log^{k-j}n}{n^s}\right).\end{aligned}$$

La suma interior es $\mathcal{O}(1)$ al ser finita y se concluye de (2.1):

$$\left|(L^*)^{(k)}(s,\chi_0)\right|\ll_k\left|(\zeta^*)^{(k)}(s)\right|\ll_k|s|\log^{k+1}(2|s|).$$

(*B*) Sea la serie que define la derivada k-ésima de $L(s,\chi)$ subdividida en dos intervalos:

$$(-1)^k L^{(k)}(s,\chi) = \sum_{n=1}^{\infty} \chi(n) \frac{\log^k n}{n^s} = \sum_{n \leq x} \chi(n) \frac{\log^k n}{n^s} + \sum_{n > x} \chi(n) \frac{\log^k n}{n^s}.$$

Para la primera suma se aplica una acotación básica:

$$\left| \sum_{n \leq x} \chi(n) \frac{\log^k n}{n^s} \right| \leq \int_1^x \frac{\log^k u}{u^\sigma} \, du \leq \log^{k+1}(x).$$

Para la segunda suma se utiliza directamente (14) y la Proposición 2.2 para deducir:

$$\sum_{n > x} \chi(n) \frac{\log^k n}{n^s} = \lim_{N \to \infty} \sum_{x < n \leq N} \chi(n) \frac{\log^k n}{n^s}$$
$$= \mathcal{O}(1) \cdot \left(\frac{\log^k N}{N^s} - \frac{\log^k x}{x^s} \right) - \int_x^N \mathcal{O}(1) \cdot \frac{k \log^{k-1} t - s \log^k t}{t^{s+1}} \, dt.$$

Analizando los términos que dependen de N, por una parte:

$$\lim_{N \to \infty} \mathcal{O}(1) \cdot \frac{\log^k N}{N^s} = 0.$$

Por otra parte, usando que $\log t = \mathcal{O}(t^\varepsilon)$ para todo $\varepsilon > 0$ y teniendo en cuenta que $\sigma > 1$, se satisface:

$$\left| \int_N^\infty \mathcal{O}(1) \cdot \frac{k \log^{k-1} t - s \log^k t}{t^{s+1}} \, dt \right| \ll N^{-\sigma + (2k-1)\varepsilon} \overset{N \to \infty}{\longrightarrow} 0,$$

por lo que se puede tomar límite en N y la integral resultante es convergente. Asimismo, para $x \geq e$ se cumple que $\log^{k-1} t \leq \log^k t$. En consecuencia, el término integral obtenido puede acotarse usando el Lema 2.13:

$$\left| \int_x^\infty \mathcal{O}(1) \cdot \frac{k \log^{k-1} t - s \log^k t}{t^{s+1}} \, dt \right| \ll_k \int_x^\infty \frac{|s| \log^k t}{t^{\sigma+1}} \, dt \ll_k |s| \frac{\log^k x}{x}.$$

También se tiene directamente para $\sigma > 1$:

$$\left| \mathcal{O}(1) \cdot \frac{\log^k x}{x^s} \right| \ll \frac{\log^k x}{x}.$$

Uniendo todas las acotaciones y sustituyendo en la expresión de $(-1)^k L^{(k)}(s,\chi)$, el resultado es:

$$(-1)^k L^{(k)}(s,\chi) = \mathcal{O}\left(\log^{k+1} x \right) + \mathcal{O}_k \left(\frac{|s| \log^k x}{x} \right).$$

Por último, tomando $x = e \cdot |s|$, se concluye:

$$(-1)^k L^{(k)}(s,\chi) = \mathcal{O}_k \left(\log^{k+1}(e|s|) \right) = \mathcal{O}_k \left(\log^{k+1}(2|s|) \right).$$

□

Proposicion 2.15 *(Cota inferior para $L(s,\chi)$) Sea $1 < \sigma < 2$.*

(*A*) *Para $\chi = \chi_0$:*

$$|L^*(s,\chi_0)| \gg (\sigma - 1)^{\frac{3}{4}} |s| \log^{-\frac{1}{4}}(2|s|).$$

(*B*) *Para $\chi \neq \chi_0$:*

$$|L(s,\chi)| \gg (\sigma - 1)^{\frac{3}{4}} \log^{-\frac{1}{4}}(2|s|).$$

Demostración.

(A) Aplicando el Lema 2.6, el producto en los primos divisores de q puede acotarse inferiormente mediante la desigualdad triangular $|1-p^{-\sigma-2it}| \geq 1-p^{-\sigma}$ obteniendo:

$$\left|\prod_{p|q}\left(1-\frac{1}{p^{\sigma+2it}}\right)\right| \geq \prod_{p|q}\left(1-\frac{1}{p^{\sigma}}\right) > \prod_{p|q}\left(1-\frac{1}{2}\right) = \left(\frac{1}{2}\right)^{\omega(q)}.$$

De esta forma, se puede deducir directamente multiplicando por $s-1$ y empleando (2.2):

$$|L^*(s,\chi_0)| \gg |\zeta^*(s)| \gg (\sigma-1)^{\frac{3}{4}}|s|\log^{-\frac{1}{4}}(2|s|).$$

(B) Véase que para $s=\sigma+it$ y para todo $\chi \neq \chi_0$ se tiene:

$$1 \leq \zeta(\sigma)^3|L(\sigma+it,\chi)|^4|L(\sigma+2it,\chi^2)|.$$

Utilizando el producto de Euler de (12) bastaría ver que para cada primo p:

$$1 \leq \left|\frac{1}{1-p^{-\sigma}}\right|^3\left|\frac{1}{1-\chi(p)p^{-\sigma-it}}\right|^4\left|\frac{1}{1-\chi^2(p)p^{-\sigma-2it}}\right|,$$

o lo que es equivalente al tomar logaritmos:

$$0 \leq 3\mathrm{Re}\left(\mathrm{Log}\left(\frac{1}{1-p^{-\sigma}}\right)\right) + 4\mathrm{Re}\left(\mathrm{Log}\left(\frac{1}{1-\chi(p)p^{-\sigma-it}}\right)\right) + \mathrm{Re}\left(\mathrm{Log}\left(\frac{1}{1-\chi^2(p)p^{-\sigma-2it}}\right)\right)$$
$$= \sum_{j=1}^{\infty}\frac{1}{j}\cdot\mathrm{Re}\left(3p^{-j\sigma}+4\chi^j(p)p^{-j(\sigma+it)}+\chi^{2j}(p)p^{-j(\sigma+2it)}\right).$$

Esta desigualdad es cierta, expresando $\chi(p)=e^{i\theta}$ para cierto θ, que cada sumando $p^{-j\sigma}(3+4\cos(j(\theta-t)\log p)+\cos(2j(\theta-t)\log p))$ es no negativo, lo cual se cumple aplicando la identidad trigonométrica $2(1+\cos(j(\theta-t)\log p))^2 = 3+4\cos(j(\theta-t)\log p)+\cos(2j(\theta-t)\log p)$. Con esto, se tiene la desigualdad de partida y basta despejar el factor $|L(s,\chi)|$ habiendo acotado superiormente los otros dos factores. Para el factor $\zeta(\sigma)$ se utiliza (2.1) para $k=0$ obteniendo:

$$\zeta(\sigma) = \frac{1}{\sigma-1}+\mathcal{O}\left(\log(2\sigma)\right) \ll \frac{1}{\sigma-1}.$$

Por otra parte, para el factor $L(\sigma+2it,\chi^2)$ hay que distinguir dos casos posibles. Si $\chi^2 \neq \chi_0$, simplemente utilizando la Proposición 2.14.(B), se puede deducir:

$$|L(\sigma+2it,\chi^2)| \ll \log(2|\sigma+2it|) \ll \log(2|s|),$$

y sustituyendo estas acotaciones y despejando $|L(s,\chi)|$, el resultado sería:

$$|L(s,\chi)| \gg (\sigma-1)^{\frac{3}{4}}\log^{-\frac{1}{4}}(2|s|).$$

Si por el contrario $\chi^2=\chi_0$ (lo que implica que χ es real no principal), en este caso vuelve a aparecer la función $\zeta(s)$ involucrada. Por el Lema 2.6, se tendría:

$$L(\sigma+2it,\chi_0) = \zeta(\sigma+2it)\prod_{p|q}\left(1-\frac{1}{p^{\sigma+2it}}\right).$$

El producto en los primos divisores de q puede acotarse superiormente así:

$$\left|\prod_{p|q}\left(1-\frac{1}{p^{\sigma+2it}}\right)\right| \leq \prod_{p|q}\left(1+\frac{1}{p^{\sigma}}\right) \leq \prod_{p|q}\left(1+\frac{1}{2}\right) = \left(\frac{3}{2}\right)^{\omega(q)}.$$

En consecuencia, empleando (2.2) y tomando $|t|>\delta>0$ para δ fijo, se obtiene:

$$|L(\sigma+2it,\chi_0)| \ll \frac{1}{2|t|}+C\log(2|s|) \ll_{\delta} \log(2|s|).$$

Sustituyendo las acotaciones y despejando $|L(s,\chi)|$, se llegaría a que existe una constante dependiente de δ tal que:

$$|L(s,\chi)| \gg_\delta (\sigma-1)^{\frac{3}{4}} \log^{-\frac{1}{4}}(2|s|).$$

Aquí es posible eliminar la dependencia de δ. La función $f(s) = (\sigma-1)^{3/4}\log^{-1/4}(2|s|)$ es continua (aunque no holomorfa) en la región compacta $\Omega = \{s \in \mathbb{C} \,|\, 1 \leq \sigma \leq 2,\ |t| \leq \delta\}$. Por tanto, $f(s)$ alcanza un máximo. Al mismo tiempo, $|L(s,\chi)|$ alcanza un mínimo no nulo también por continuidad en Ω, ya que por la Proposición 2.5 $L(1,\chi) \neq 0$ y $L(s,\chi)$ no se anula para $\sigma > 1$. Por tanto, puede ajustarse δ de forma que la constante de acotación sea absoluta y así, para $1 < \sigma < 2$ se concluye:

$$|L(s,\chi)| \gg (\sigma-1)^{\frac{3}{4}} \log^{-\frac{1}{4}}(2|s|).$$

□

D. Demostración del Teorema de los Números Primos en Progresiones Aritméticas. Una vez constatados los requisitos técnicos previos y las acotaciones para las funciones $L(s,\chi)$, ya es posible probar el resultado central de este Capítulo, el cual responderá a la última cuestión planteada al final de la Sección 1. En el argumento que siguió Iwaniec en su prueba del *Teorema de los Números Primos* en la forma $M(x) = o(x)$, aunque la asintótica $\zeta(s) \sim (s-1)^{-1}$ aparece de una forma u otra en todas las acotaciones y como se ha dicho es importante, lo crucial e ingenioso en la idea de Iwaniec es el hecho de que al tomar derivadas sucesivas consigue una mejora creciente en el orden de derivación k para las sumas regularizadas:

$$\sum_{n\leq x} \mu(n)\log^k n \log\frac{x}{n}$$

si se compara con una cota trivial que correspondería a $\mathcal{O}(x\log^k x)$. Cuando la mejora es suficientemente buena es posible eliminar la regularización $\log(x/n)$, de tal forma que obtener la función $M(x)$ es solo sumar por partes. Extender esta idea a las funciones $L(s,\chi)$ se traduce en lo siguiente:

Teorema 2.16 (G.,2018) *(Versión del Teorema de los Números Primos en Progresiones Aritméticas) Sea χ un caracter de Dirichlet módulo q. Entonces:*

$$\lim_{x\to+\infty} \frac{1}{x}\sum_{n\leq x} \chi(n)\mu(n) = 0.$$

Más concretamente,

$$M_\chi(x) = \mathcal{O}\left(x\log^{-A} x\right),$$

donde la constante implícita depende de q.

Demostración. Sea la función:

$$G_\chi(s) = (-1)^k \left(\frac{1}{L}\right)^{(k)}(s,\chi).$$

$G_\chi(s)$ tiene la siguiente expresión en forma de serie:

$$G_\chi(s) = (-1)^k \frac{d^k}{ds^k}\left(\sum_{n=1}^{\infty}\frac{\chi(n)\mu(n)}{n^s}\right) = \sum_{n=1}^{\infty}\chi(n)\mu(n)\frac{\log^k n}{n^s}.$$

Sea también la función:

$$F_\chi(x) = \sum_{n\leq x}\chi(n)\mu(n)\log^k n\log\frac{x}{n}.$$

La estrategia de la prueba es estimar F_χ a través de G_χ de forma suficientemente adecuada y de ahí obtener la estimación para la suma del enunciado. El primer objetivo es encontrar una relación entre F_χ y G_χ. Como primer paso, se tiene la siguiente acotación:

$$\left|\frac{x^s}{s^2}\sum_{n=1}^{N}\chi(n)\mu(n)\frac{\log^k n}{n^s}\right| \leq \frac{x^\sigma}{\sigma^2+t^2}\sum_{n=1}^{N}\frac{\log^k n}{n^\sigma}.$$

La serie que mayora converge uniformemente en compactos, por lo que al tomar límite en N es posible intercambiar la serie y la integral y haciendo uso de la Proposición 2.10, se deduce:

$$\begin{aligned}\frac{1}{2\pi i}\int_{\mathrm{Re}(s)=\sigma} G_\chi(s)\cdot\frac{x^s}{s^2}\,ds &= \frac{1}{2\pi i}\int_{\mathrm{Re}(s)=\sigma}\sum_{n=1}^{\infty}\chi(n)\mu(n)\frac{\log^k n}{n^s}\cdot\frac{x^s}{s^2}\,ds\\ &= \sum_{n=1}^{\infty}\chi(n)\mu(n)\log^k n\cdot\frac{1}{2\pi i}\int_{\mathrm{Re}(s)=\sigma}\left(\frac{x}{n}\right)^s\cdot\frac{ds}{s^2} = \sum_{n=1}^{\infty}\chi(n)\mu(n)\log^k n\left(\log\frac{x}{n}\right)_+ = F_\chi(x).\end{aligned}$$

Una vez se ha establecido la relación entre F_χ y G_χ, se aplica la *Fórmula de Faà di Bruno* (Teorema 2.12.(B)) a las funciones $L(s,\chi)$ para $\chi\neq\chi_0$ y $L^*(s,\chi_0)$. Para las primeras, se utilizan las cotas superiores de sus derivadas (Proposición 2.14.(B)) y la cota inferior de la propia función (Proposición 2.15.(B)). Más concretamente:

$$\left|\frac{1}{L(s,\chi)}\right| \ll (\sigma-1)^{-\frac{3}{4}}\log^{\frac{1}{4}}(2|s|), \qquad \left|\frac{L^{(j)}(s,\chi)}{L(s,\chi)}\right| \ll_j (\sigma-1)^{-\frac{3}{4}}\log^{j+\frac{5}{4}}(2|s|), \quad 1\leq j\leq k.$$

De esta forma, $G_\chi(s)$ para $\chi\neq\chi_0$ se puede estimar de la siguiente forma:

$$\begin{aligned}|G_\chi(s)| &= \left|\frac{(-1)^k}{L(s,\chi)}\sum_{a_1+\ldots+ka_k=k} C_{a_1,\ldots,a_k}\prod_{j=1}^{k}\frac{L^{(j)}(s,\chi)}{L(s,\chi)}\right|\\ &\ll_k (\sigma-1)^{-\frac{3}{4}-\frac{3}{4}\sum a_j}\log^{\frac{1}{4}+k+\frac{5}{4}\sum a_j}(2|s|) \overset{[2]}{\leq} (\sigma-1)^{-\frac{3}{4}(k+1)}\log^{\frac{9k+1}{4}}(2|s|).\end{aligned}$$

Se procede ahora de forma análoga para $L^*(s,\chi_0)$, utilizando las cotas superiores de sus derivadas (Proposición 2.14.(A)) y la cota inferior de la propia función (Proposición 2.15.(A)). Más concretamente:

$$\left|\frac{1}{L^*(s,\chi_0)}\right| \ll (\sigma-1)^{-\frac{3}{4}}|s|^{-1}\log^{\frac{1}{4}}(2|s|), \qquad \left|\frac{(L^*)^{(j)}(s,\chi_0)}{L^*(s,\chi_0)}\right| \ll_j (\sigma-1)^{-\frac{3}{4}}\log^{j+\frac{5}{4}}(2|s|), \quad 1\leq j\leq k.$$

Empleando de nuevo la *Fórmula de Faà di Bruno* (Teorema 2.12.(B)) se llega a:

$$\begin{aligned}\left|\left(\frac{1}{L^*(s,\chi_0)}\right)^{(k)}\right| &= \left|\frac{1}{L^*(s,\chi_0)}\sum_{a_1+\ldots+ka_k=k} C_{a_1,\ldots,a_k}\prod_{j=1}^{k}\frac{(L^*)^{(j)}(s,\chi_0)}{L^*(s,\chi_0)}\right|\\ &\ll_k (\sigma-1)^{-\frac{3}{4}-\frac{3}{4}\sum a_j}|s|^{-1}\log^{\frac{1}{4}+k+\frac{5}{4}\sum a_j}(2|s|) \leq (\sigma-1)^{-\frac{3}{4}(k+1)}|s|^{-1}\log^{\frac{9k+1}{4}}(2|s|).\end{aligned}$$

Una vez hecho esto, es posible utilizar la definición de $L^*(s,\chi_0)$, la *Regla de Leibniz* y el que $|1/s|<1$ cuando $\sigma>1$ para que $G_{\chi_0}(s)$ se puede estimar de la siguiente forma:

$$\begin{aligned}\left|(-1)^kG_{\chi_0}(s)\right| &= \left|(s-1)\left(\frac{1}{L^*(s,\chi_0)}\right)^{(k)} + k\left(\frac{1}{L^*(s,\chi_0)}\right)^{(k-1)}\right|\\ &\ll_k \left|\frac{s-1}{s}\right|(\sigma-1)^{-\frac{3}{4}(k+1)}\log^{\frac{9k+1}{4}}(2|s|) + k(\sigma-1)^{-\frac{3}{4}k}|s|^{-1}\log^{\frac{9k-8}{4}}(2|s|)\\ &\leq (\sigma-1)^{-\frac{3}{4}(k+1)}\log^{\frac{9k+1}{4}}(2|s|)\left(2+k(\sigma-1)^{\frac{3}{4}}\log^{-\frac{9}{4}}(2|s|)\right)\\ &\ll_k (\sigma-1)^{-\frac{3}{4}(k+1)}\log^{\frac{9k+1}{4}}(2|s|).\end{aligned}$$

La conclusión a la que se llega es que independientemente de quien sea χ, es posible obtener la misma acotación para $G_\chi(s)$, por lo que a partir de aquí se volverá a considerar un caracter χ general. El siguiente paso es hacer uso de la estimación de $G_\chi(s)$ y la relación entre $F_\chi(x)$ y $G_\chi(s)$ para poder realizar la estimación correspondiente de $F_\chi(x)$. Así:

$$\begin{aligned}|F_\chi(x)| &= \left|\frac{1}{2\pi i}\int_{\mathrm{Re}(s)=\sigma} G_\chi(s)\cdot\frac{x^s}{s^2}\,ds\right| \ll \int_{\mathrm{Re}(s)=\sigma} x^\sigma|G_\chi(s)|\cdot\left|\frac{ds}{s^2}\right|\\ &\ll_k x^\sigma(\sigma-1)^{-\frac{3}{4}(k+1)}\int_{\mathrm{Re}(s)=\sigma}\log^{\frac{9k+1}{4}}(2|s|)\left|\frac{ds}{s^2}\right|.\end{aligned}$$

[2] Para simplificar los exponentes se tiene en cuenta que $\sum a_j\leq k$ y si $0<x<1$, entonces $x^{-n}\leq x^{-m}$ para $m>n>0$.

Para la integral que se ha obtenido se sigue lo siguiente:

$$\int_{\mathrm{Re}(s)=\sigma} \log^{\frac{9k+1}{4}}(2|s|)\left|\frac{ds}{s^2}\right| = \int_{-\infty}^{+\infty} \frac{\log^{\frac{9k+1}{4}}(2\sqrt{\sigma^2+t^2})}{\sigma^2+t^2}\,dt$$
$$\ll \int_{-\infty}^{+\infty} \frac{\log^{\frac{9k+1}{4}}(1+|t|)}{1+t^2}\,dt \ll \int_0^{\infty} \frac{dt}{(1+t^2)^{1-\varepsilon}} = \mathcal{O}(1).$$

Esto quiere decir que para $1<\sigma<2$:

$$F_\chi(x) = \mathcal{O}_k\left(x^\sigma(\sigma-1)^{-\frac{3}{4}(k+1)}\right).$$

Eligiendo ahora $\sigma = 1+1/\log x$ entonces $1<\sigma<2$ implica que $x>e$. Esta elección no implica pérdida de información, ya que si $x\leq e$ la estimación de vuelve trivial (de hecho, $F_\chi(x)=0$ para $x<2$). Así, sustituyendo el valor de σ se verifica:

$$F_\chi(x) = \mathcal{O}_k\left(x^{1+\frac{1}{\log x}}\log^{\frac{3}{4}(k+1)}x\right) = \mathcal{O}_k\left(x\log^{\frac{3}{4}(k+1)}x\right).$$

Para finalizar la demostración, se recupera la suma del enunciado a través de otra función auxiliar. Sea:

$$H_\chi(x) = \sum_{m\leq x}\chi(m)\mu(m)\log^k m.$$

Para $y\leq x$ se cumple:

$$F_\chi(x+y)-F_\chi(x) = \sum_{m\leq x+y}\chi(m)\mu(m)\log^k m\log\frac{x+y}{m} - \sum_{m\leq x}\chi(m)\mu(m)\log^k m\log\frac{x}{m}$$
$$= \sum_{m\leq x}\chi(m)\mu(m)\log^k m\left(\log\frac{x+y}{m}-\log\frac{x}{m}\right) + \sum_{x<m\leq x+y}\chi(m)\mu(m)\log^k m\log\frac{x+y}{m}$$
$$= H_\chi(x)\log\frac{x+y}{x} + \sum_{x<m\leq x+y}\chi(m)\mu(m)\log^k m\log\frac{x+y}{m}.$$

Se tiene $\log(x+y)\ll\log x$, por lo que la segunda suma verifica:

$$\left|\sum_{x<m\leq x+y}\chi(m)\mu(m)\log^k m\log\frac{x+y}{m}\right| \leq \sum_{x<m\leq x+y}\log^k m\log\frac{x+y}{m} \ll y\log^k x\log\frac{x+y}{x}.$$

En consecuencia:

$$F_\chi(x+y)-F_\chi(x) = H_\chi(x)\log\frac{x+y}{x} + \mathcal{O}\left(y\log^k x\log\frac{x+y}{x}\right),$$

y puesto que $\log((x+y)/x)\gg y/x$, recurriendo a la estimación de $F_\chi(x)$, se deduce:

$$H_\chi(x) \ll_k y\log^k x + \frac{x}{y}\left((x+y)\log^{\frac{3}{4}(k+1)}(x+y) + x\log^{\frac{3}{4}(k+1)}x\right) = y\log^k x + \frac{x^2}{y}\log^{\frac{3}{4}(k+1)}x.$$

Optimizando esta cota igualando ambos sumandos y despejando y, la estimación final de $H_\chi(x)$ es:

$$H_\chi(x) = \mathcal{O}_k\left(x\log^{k-A}x\right), \quad A=\frac{k-3}{8}.$$

De aquí se obtiene el *Teorema de los Números Primos en Progresiones Aritméticas* simplemente empleando (14) y la estimación de $H_\chi(x)$:

$$\sum_{n\leq x}\chi(n)\mu(n) = \sum_{n\leq x}\chi(n)\mu(n)\log^k x\cdot\frac{1}{\log^k x} = \frac{H_\chi(x)}{\log^k x} - \frac{H_\chi(2)}{\log^k 2} + k\int_2^x \frac{H_\chi(t)}{t\log^{k+1}t}\,dt$$
$$\ll_k x\log^{-A}x + k\int_2^x \log^{-A-1}t\,dt \ll_k x\log^{-A}x.$$

Dividiendo entre x y tomando límite se concluye:

$$\lim_{x\to+\infty}\frac{1}{x}\sum_{n\leq x}\chi(n)\mu(n) = 0,$$

ya que al ser k un número arbitrario, A es arbitrario y basta tomar $k>3$ para que A sea positivo y produzca una buena estimación. □

Capítulo 3

Una de las últimas conjeturas de Javier Cilleruelo

§1. Planteamiento de la conjetura de Javier Cilleruelo

A. Introducción. El problema que se va a tratar en este Capítulo parte de un planteamiento muy sencillo. Dado un entero positivo n, cada divisor $d \mid n$ puede ser sumado con su correspondiente divisor complementario n/d y haciendo esto con todos los divisores se obtiene el conjunto de números:

$$S(n) := \{d + n/d \,:\, d \mid n\}.$$

Aunque este conjunto a primera vista puede parecer completamente aleatorio e irrelevante, observando los números que aparecen es posible apreciar que para algunos n ocurre un fenómeno aritmético curioso en sus respectivos $S(n)$: la presencia de números consecutivos. Observando diversos ejemplos, no parece haber a simple vista un patrón o una fórmula para los n de partida, y aparte de ello, la cantidad de números consecutivos que se aprecian es variable, teniéndose por ejemplo:

$$S(4) = \{\mathbf{4}, \mathbf{5}\}, \qquad S(144) = \{\mathbf{24}, \mathbf{25}, \mathbf{26}, 30, 40, 51, 74, 145\},$$

$$\begin{aligned} S(15120) = \{&\mathbf{246}, \mathbf{247}, \mathbf{248}, \mathbf{249}, 258, 264, 269, 282, 286, 303, 312, 326, 334, 363,\\ &381, 402, 418, 456, 467, 534, 568, 587, 654, 741, 776, 858, 961, 1023,\\ &1094, 1272, 1522, 1689, 1898, 2167, 2526, 3029, 3784, 5043, 7562, 15121\}. \end{aligned}$$

A pesar de esta incertidumbre, en este Capítulo se dará respuesta a los interrogantes anteriores en un intento de aclarar y formalizar el porqué de este fenómeno aritmético. Más concretamente, dado $K \geq 2$ entero positivo, se considera el conjunto:

$$\mathcal{S}_K = \left\{n \in \mathbb{Z}^+ \,:\, S(n) \text{ contiene } K \text{ enteros consecutivos}\right\}.$$

En este sentido, el profesor Javier Cilleruelo enunció la que es la conjetura principal de este Capítulo:

Conjetura 3.1 (Cilleruelo) *El conjunto $\mathcal{S}_K$ es infinito para $2 \leq K \leq 4$ y es vacío para $K \geq 5$.*

La motivación de este problema no surge de la nada. En [**?**], Erdös y Rosenfeld enunciaron una conjetura concerniente a un conjunto diferente a $S(n)$:

Conjetura 3.2 (Erdös, Rosenfeld) *Sea el conjunto de diferencias de divisores complementarios:*

$$D(n) := \{|n/d - d| \,:\, d \mid n\}.$$

Entonces para cada $K \in \mathbb{Z}^+$ existen enteros positivos $N_1 < \ldots < N_K$ tales que

$$\left|\bigcap_{j=1}^{K} D(N_j)\right| \geq K.$$

Independientemente de la analogía de los conjuntos $S(n)$ y $D(n)$, Javier Cilleruelo seguramente expuso la Conjetura 3.1 más motivado por sus trabajos sobre puntos del retículo (de coordenadas enteras) y divisores [**?**], [**?**] que por la Conjetura 3.2. Un indicio de ello podría ser que ambas conjeturas no tienen mucho que ver en el sentido de que la segunda pide elementos coincidentes en muchos $D(n)$, mientras que la primera habla de infinitos $S(n)$ no relacionados que satisfagan una propiedad común. Al margen de esto, es posible ofrecer una visión geométrica de la Conjetura 3.1 como el problema consistente esencialmente en encontrar el máximo número de rectas $x+y=k$ con $k \in \mathbb{Z}^+$ que cortan a la hipérbola $xy=n$ en puntos del retículo. Sin embargo, no ha quedado claro si este enfoque distinto formaba parte o no de la visión de Javier Cilleruelo sobre el problema.

Como se ha señalado anteriormente, el fenómeno de los números consecutivos no ofrece patrones visibles a simple vista. Buscando evidencia numérica, si se computa el conjunto $S(n)$ para un rango extenso de n, se puede apreciar bastante irregularidad, siendo $n=4$ el primer elemento de $\mathcal{S}_2$, $n=144$ el primer elemento de $\mathcal{S}_3$ y $n=15120$ el primer elemento de $\mathcal{S}_4$. Sin embargo, lo único que puede percibirse es que puede parecer que los términos consecutivos corresponden siempre a las sumas más pequeñas, originadas por los divisores más cercanos a $\sqrt{n}$. Desafortunadamente, esto no es completamente cierto, ya que por ejemplo, para $n=1024382594995200$ se tiene:

$$S(1024382594995200) = \{64011955, 64011956, \mathbf{64011966}, \mathbf{64011967}, \mathbf{64011968}, 64012452,$$
$$64013320, 64013612, 64013880, 64015120, 64015905, 64019920, \ldots\}.$$

En cuanto a la Conjetura 3.1, la evidencia numérica revela únicamente cómo la proporción de números desciende notablemente cuando K aumenta y hasta la fecha no se ha encontrado ningún elemento de $\mathcal{S}_5$ en un rango aproximado de n en torno a unas 30 cifras, lo cual solo indica que si los hubiera, el primero de ellos debe ser un número considerablemente grande.

B. Ecuaciones diofánticas. La Conjetura 3.1 está fuertemente relacionada con la existencia de soluciones de ciertas ecuaciones cuadráticas diofánticas. Para llegar a establecer dicha relación, se parte del siguiente resultado:

Lema 3.3 *Dado $d \in \mathbb{Z}^+$, cierto $n \in \mathbb{Z}^+$ verifica que existen dos divisores positivos d_1, $d_2 \mid n$ tales que $d_2 + n/d_2 - (d_1 + n/d_1) = d$ si y solo si $n = ab(a-f_1)(b-f_2)$ con $f_1 f_2 = d$ y a, b, $a-f_j$, $f_j \in \mathbb{Z}^+$. De hecho, pueden tomarse $d_1 = (a-f_1)b$ y $d_2 = ab$.*

Demostración. Cambiando d_1 por n/d_1 y d_2 por n/d_2 si es necesario, se puede suponer sin pérdida de generalidad que $d_2 > d_1$. Sea $a = \mathrm{mcd}(d_1, d_2)$ y sean $d_2 = ab$ y $d_1 = ab'$. Entonces:

$$d = d_2 + \frac{n}{d_2} - \left(d_1 + \frac{n}{d_1}\right) = \left(a - \frac{n}{abb'}\right)(b - b'),$$

donde ambos factores del producto son positivos, díganse f_1 y f_2. Eliminando b' en el sistema de ecuaciones $a - n/(abb') = f_1$ y $b - b' = f_2$, se concluye que $n = ab(a-f_1)(b-f_2)$. Recíprocamente, si se toman $d_1 = b(a-f_1)$ y $d_2 = ab$, entonces:

$$d_1 + \frac{n}{d_1} = b(a-f_1) + a(b-f_2) = 2ab - af_2 - bf_1, \qquad d_2 + \frac{n}{d_2} = ab + (a-f_1)(b-f_2) = 2ab - af_2 - bf_1 + f_1 f_2,$$

y su diferencia satisface $d_2 + n/d_2 - (d_1 + n/d_1) = f_1 f_2 = d$. □

Este resultado permite dar una caracterización directa para el conjunto $\mathcal{S}_2$:

Corolario 3.4 $\mathcal{S}_2 = \{ab(a-1)(b-1) \,:\, a,\, b \in \mathbb{Z}_{>1}\}$.

Demostración. Basta tomar $d=1$ en el Lema 3.3 y observar que si $a=1$ o $b=1$, entonces $n=0$. □

La caracterización del conjunto $\mathcal{S}_3$ proviene también del Lema 3.3 pero no es tan directa como en el caso de $\mathcal{S}_2$:

Proposicion 3.5 *Se verifica:*

$$\mathcal{S}_3 = \left\{ \frac{1}{4}(x^2-1)(y^2-1) \,:\, x^2+y^2-1 = z^2 \text{ con } x, y, z \in \mathbb{Z}_{>1} \right\}.$$

Demostración. Por definición, $n \in \mathcal{S}_3$ si y solo si existen divisores positivos d_1, d_2, $d_3 \mid n$ tales que:

$$d_3 + \frac{n}{d_3} - \left(d_1 + \frac{n}{d_1}\right) = 2, \qquad d_2 + \frac{n}{d_2} - \left(d_1 + \frac{n}{d_1}\right) = 1.$$

Aplicando el Lema 3.3 para $d = 2$ se obtiene $n = a(a-1)b(b-2)$ y escribiendo $a = (x+1)/2$, $b = y+1$ con x, $y \in \mathbb{Z}_{>1}$ y $x \in \mathbb{O}$ se deduce que $n = (x^2-1)(y^2-1)/4$, siendo $d_1 = (x-1)(y-1)/2$. Como $d_1 + n/d_1 = xy - 1$, entonces $d_2 + n/d_2 = xy$, por lo que $X = d_2$ y $X = n/d_2$ son las raíces de la ecuación cuadrática $X^2 - xyX + n = 0$ (ya que su suma es xy y su producto es n). Para que la ecuación posea raíces racionales, el discriminante Δ debe ser un cuadrado, es decir, $\Delta = x^2y^2 - 4n = x^2y^2 - (x^2-1)(y^2-1) = x^2 + y^2 - 1 = z^2$. Además $z \in \mathbb{Z}_{>1}$. De aquí se deduce la inclusión:

$$\mathcal{S}_3 \subseteq \left\{ \frac{1}{4}(x^2-1)(y^2-1) \,:\, x^2+y^2-1 = z^2 \text{ con } x,y,z \in \mathbb{Z}_{>1} \right\}.$$

Para probar la inclusión contraria, si $x^2 + y^2 - 1 = z^2$, al ser $z^2 \equiv 0, 1 \pmod 4$ para todo z, entonces $x^2 + y^2 \equiv 0 \pmod 4$. Esto implica que forzosamente o bien x es impar o bien y es impar. Si uno de ellos es par y el otro impar, entonces z es par. Si por el contrario ambos son impares, entonces z es impar. En cualquiera de los dos casos se llega a que $xy + z$ es par. Despejando de la ecuación $\Delta = z^2$, $d_2 = (xy+z)/2$ (puede tomarse también $d_2 = (xy-z)/2$). Con esto se concluye que d_1, d_2 y $d_3 = (x+1)(y+1)/2$ son enteros positivos divisores de $n = (x^2-1)(y^2-1)/4$ cuyas sumas $d_j + n/d_j$ son los números consecutivos $xy-1$, xy y $xy+1$. □

Una vez formalizado el caso $K = 3$, el caso general $K > 3$ consiste esencialmente en una aplicación repetida de la última parte en la demostración de la Proposición 3.5:

Proposicion 3.6 *Para $K > 3$, $n \in \mathcal{S}_K$ si y solo si $n = (x^2-1)(y^2-1)/4$ para ciertos x, $y \in \mathbb{Z}_{>1}$ tales que $x^2 + 2(k-2)xy + y^2 + k^2 - 4k + 3$ son cuadrados para $k = 2$ y $3 < k \leq K$.*

Demostración. Por la Proposición 3.5, el resultado ya se tiene para $K = 3$, encontrando divisores d_k tales que $d_k + n/d_k = xy + k - 2$ para $1 \leq k \leq 3$. Por tanto, basta encontrar condiciones necesarias y suficientes para que esto se satisfaga para $3 < k \leq K$, lo cual puede establecerse imponiendo que las ecuaciones cuadráticas $X^2 - (xy + k - 2)X + n = 0$ tengan soluciones enteras para $3 < k \leq K$, ya que dichas soluciones proporcionan elecciones válidas para d_k y n/d_k. De hecho, las soluciones serán en efecto enteras si y solo si el discriminante $\Delta = (xy + k - 2)^2 - 4n$ es un cuadrado y tiene la misma paridad que $xy + k - 2$. Esta última condición es trivial, ya que ambas cantidades son congruentes módulo 2, y la primera condición se cumple al desarrollar Δ y sustituir $n = (x^2-1)(y^2-1)/4$, obteniendo $\Delta = (xy+k-2)^2 - (x^2-1)(y^2-1) = x^2+y^2+2(k-2)xy+k^2-4k+3$.□

Como consecuencia de este resultado, las ecuaciones del caso $K = 4$ corresponden a:

$$(K4) \qquad x^2 + y^2 = z_0^2 + 1, \qquad x^2 + 4xy + y^2 = z_1^2 - 3,$$

mientras que las del caso $K = 5$ corresponden a:

$$(K5) \qquad x^2 + y^2 = z_0^2 + 1, \qquad x^2 + 4xy + y^2 = z_1^2 - 3, \qquad x^2 + 6xy + y^2 = z_2^2 - 8.$$

En ambos casos, se dirá que una solución de las ecuaciones es *no trivial* si x^2, $y^2 \neq 1$. De esta forma se obtiene otra caracterización de la Conjetura 3.1, mucho más práctica a la hora de trabajar:

Corolario 3.7 *La Conjetura 3.1 es cierta si y solo si $(K4)$ tiene infinitas soluciones con x, $y \in \mathbb{Z}_{>1}$ y $(K5)$ no tiene ninguna.*

La Proposición 3.6 exige que x, $y \in \mathbb{Z}_{>1}$. Observando a simple vista las ecuaciones $(K4)$, es posible establecer simetrías como el intercambio de ciertas variables o cambios de signo en las tuplas de soluciones enteras (x, y, z_0, z_1) para generar soluciones no triviales. Sin embargo, existen simetrías más complejas que también ejercen esta función y que no son observables a simple vista. Como muestra de ello:

Proposicion 3.8 *Sean las aplicaciones lineales que actúan sobre las tuplas $\vec{w} = (x, y, z_0, z_1)$:*

$$L_1(\vec{w}) = (y, x, z_0, z_1), \qquad L_2(\vec{w}) = (-x, -y, z_0, z_1), \qquad L_3(\vec{w}) = (x, y, -z_0, z_1), \qquad L_4(\vec{w}) = (x, y, z_0, -z_1),$$

$$L_5(\vec{w}) = \left(-\frac{z_0 + z_1}{2}, -\frac{z_0 - z_1}{2}, -x - y, -x + y \right);$$

y sea G el grupo generado por ellas. Entonces G deja invariante el conjunto de soluciones de $(K4)$ y para cualquier solución no trivial $\vec{w} \in \mathbb{Z}^4$ existe $L \in G$ tal que $L(\vec{w}) \in (\mathbb{Z}_{>1})^4$.

Demostración. Es obvio que las aplicaciones L_j para $1 \leq j \leq 4$ dejan invariantes las soluciones de $(K4)$. Aplicando L_5, se obtienen las ecuaciones $F_1 = 0$ y $F_2 = 0$, siendo:

$$F_1 := \frac{z_0^2 + z_1^2}{2} - (x^2 + 2xy + y^2 + 1), \qquad F_2 := \frac{z_0^2 + z_1^2}{2} + z_0^2 - z_1^2 - (x^2 - 2xy + y^2 - 3).$$

Así, las ecuaciones $(F_1 + F_2)/2 = 0$ y $(3F_1 - F_2)/2 = 0$ dan lugar a $(K4)$. Por otra parte, si $\vec{w} = (x, y, z_0, z_1)$ es una solución no trivial, aplicando L_2, L_3 y L_4 es posible suponer sin pérdida de generalidad que z_0, $z_1 \in \mathbb{Z}_{\geq 0}$ y $x \in \mathbb{Z}_{>1}$. Si $y \in \mathbb{Z}_{>1}$, entonces $\vec{w} \in (\mathbb{Z}_{>1})^4$ directamente. Si $y = 0$, al sustituir en las ecuaciones de $K = 4$ se obtiene $(z_1 - z_0)(z_1 + z_0) = 4$, de donde o bien $z_1 - z_0 = \pm 1$ y $z_1 + z_0 = \pm 4$ (lo cual lleva a que z_0, $z_1 \notin \mathbb{Z}$) o bien $z_1 - z_0 = 2$ y $z_1 + z_0 = 2$ (lo cual lleva a que $x^2 = 1$). En ambos casos hay contradicción con que $\vec{w}$ sea una solución no trivial. Por último, sea $y \in \mathbb{Z}_{<-1}$. En este caso $x^2 + y^2 \geq 8$, por lo que $z_0 > 2$ y así $z_0 + z_1 > 2$. Al restar las ecuaciones se obtiene $4(xy + 1) = z_1^2 - z_0^2$. Por tanto, $2 \mid z_0 - z_1$ y $z_0 - z_1 \geq 2$. De hecho, $z_0 - z_1 > 2$ ya que si se tuviera $z_0 - z_1 = 2$, ello implicaría que $z_0 = 2 + z_1$ y al sustituir en $(K4)$ se tendría $z_1 = -xy - 2$ y de ahí que $x^2 + y^2 - 1 = x^2 y^2$ lo cual es imposible para $x \in \mathbb{Z}_{>1}$ e $y \in \mathbb{Z}_{<-1}$. Una vez que se ha deducido que $z_0 \pm z_1 > 2$ y $2 \mid z_0 - z_1$, entonces:

$$(L_2 \circ L_5)(\vec{w}) = \left(\frac{z_0 + z_1}{2}, \frac{z_0 - z_1}{2}, -x - y, -x + y \right) = (x', y', z_0', z_1'),$$

donde x', $y' \in \mathbb{Z}_{>1}$ y a través de L_3 y L_4 es posible ajustar el signo de z_0' y z_1' para que se concluya que $(L_2 \circ L_5)(\vec{w}) \in (\mathbb{Z}_{>1})^4$. □

Con este resultado, el Corolario 3.7 puede precisarse un poco más:

Corolario 3.9 *Si $(K4)$ posee infinitas soluciones no triviales y $(K5)$ no posee ninguna, entonces la Conjetura 3.1 es cierta. Se tiene el recíproco en el caso de $(K4)$.*[1]

El grupo $G = \langle L_1, L_2, L_3, L_4, L_5 \rangle$ es de orden 32 y es isomorfo al producto semidirecto $C_2^4 \rtimes C_2$, donde los factores corresponden a $C_2^4 \cong \langle L_1, L_2, L_3, L_4 \rangle$ y $C_2 \cong \langle L_5 \rangle$. Además, una vez que se especifica el orden de las dos primeras coordenadas de $L(\vec{w})$ puede comprobarse que L es única. En efecto, si para cierto $\vec{w}$ solución no trivial y ciertas L, $L' \in G$ se satisficiera $L(\vec{w}) \in (\mathbb{Z}_{>1})^4$ y $L'(\vec{w}) \in (\mathbb{Z}_{>1})^4$ pero $L \neq L'$, entonces denotando $\vec{u} := L(\vec{w})$ se seguiría que $L'(L^{-1}(\vec{u})) \in (\mathbb{Z}_{>1})^4$, donde $\tilde{L} := L'L^{-1} \neq \mathrm{Id}$. Sin embargo, esta última deducción, una vez establecido el orden de las variables (es decir, salvo aplicar L_1) no puede ser posible. Para comprobarlo basta ver que toda $\tilde{L}(\vec{u}) = (\tilde{x}, \tilde{y}, \tilde{z}_0, \tilde{z}_1)$ posee al menos una componente negativa cuando $\vec{u} \in (\mathbb{Z}_{>1})^4$. Gracias a la conmutatividad de las L_j para $1 \leq j \leq 4$ y al ser G isomorfo a un producto semidirecto [2], $\tilde{L}$ puede expresarse una vez especificado el orden las dos primeras componentes como $L_2^{\alpha_2} L_3^{\alpha_3} L_4^{\alpha_4} L_5^{\gamma}$ con $\alpha_j, \gamma \in \{0, 1\}$. Restando las ecuaciones de $(K4)$, se obtiene la identidad $4xy + 2 = z_1^2 - z_0^2$. Por tanto, si todas las componentes de $\vec{u}$ son positivas, entonces $z_1 > z_0$. Teniendo esto en cuenta y analizando todas las posibilidades para $\tilde{L}$, se obtiene la siguiente tabla de signos:

$(\alpha_2, \alpha_3, \alpha_4, \gamma)$	$\tilde{x}$	$\tilde{y}$	$\tilde{z}_0$	$\tilde{z}_1$	$(\alpha_2, \alpha_3, \alpha_4, \gamma)$	$\tilde{x}$	$\tilde{y}$	$\tilde{z}_0$	$\tilde{z}_1$
$(0,0,0,0)$	$+$	$+$	$+$	$+$	$(0,0,0,1)$	$-$	$+$	$-$	?
$(1,0,0,0)$	$-$	$-$	$+$	$+$	$(1,0,0,1)$	$-$	$+$	$+$	?
$(0,1,0,0)$	$+$	$+$	$-$	$+$	$(0,1,0,1)$	$-$	$+$	$-$	?
$(0,0,1,0)$	$+$	$+$	$+$	$-$	$(0,0,1,1)$	$+$	$-$	$-$	?
$(1,1,0,0)$	$-$	$-$	$-$	$+$	$(1,1,0,1)$	$-$	$+$	$+$	?
$(1,0,1,0)$	$-$	$-$	$+$	$-$	$(1,0,1,1)$	$+$	$-$	$+$	?
$(0,1,1,0)$	$+$	$+$	$-$	$-$	$(0,1,1,1)$	$+$	$-$	$-$	?
$(1,1,1,0)$	$-$	$-$	$-$	$-$	$(1,1,1,1)$	$+$	$-$	$+$	?

Las interrogaciones (?) indican que el signo es indeterminado (dependiendo del valor de las componentes de $\vec{u}$ involucradas, puede ser positivo o negativo). Como puede observarse, salvo para $\tilde{L} = \mathrm{Id}$, el resto de combinaciones siempre origina al menos una componente negativa. Con esto quedaría probada la unicidad de L en el sentido

[1] Los resultados anteriores exigen x, $y \in \mathbb{Z}_{>1}$, pero en $(K5)$ puede darse el caso de que todas las soluciones no triviales siempre tengan una variable negativa. Como esta situación no está recogida en los resultados anteriores, entonces el recíproco en el caso de $(K5)$ no tiene por qué ser cierto.

[2] Al ser G isomorfo a un producto semidirecto $G_1 \rtimes G_2$, todo elemento $g \in G$ puede escribirse como $g = g_1 g_2$, donde $g_j \in G_j$ para $j = 1, 2$. Una manera efectiva de verlo es que las relaciones $L_5 L_1 = L_4 L_5$, $L_5 L_2 = L_3 L_4 L_5$, $L_5 L_3 = L_1 L_2 L_5$ y $L_5 L_4 = L_1 L_5$ implican que siempre existen β_1, $\beta_2\, \beta_3\, \beta_4 \in \{0, 1\}$ tales que $L_5^{\gamma} L_1^{\alpha_1} L_2^{\alpha_2} L_3^{\alpha_3} L_4^{\alpha_4} = L_1^{\beta_1} L_2^{\beta_2} L_3^{\beta_3} L_4^{\beta_4} L_5^{\gamma}$.

comentado.

A partir de la presencia de L_5, es posible notar que partiendo de una solución $(x, y, z_0, z_1) \in (\mathbb{Z}^+)^4$ de $(K4)$, L_5 dará una solución $x < 0 < y$. Por tanto, L_5 establece una simetría entre soluciones válidas (con x e y positivas) y no válidas (con x e y de distinto signo). Por tanto, como cambiar el signo de los z_j no aporta nada nuevo y L_5 no ofrece nuevas soluciones válidas, es natural considerar soluciones salvo simetrías.

§2. Estructura de los conjuntos $\mathcal{S}_K$ para $2 \leq K \leq 4$

A. Caracterización de $\mathcal{S}_2$ y $\mathcal{S}_3$. La caracterización dada por el Corolario 3.4 ofrece una fórmula para generar fácilmente cuantos números en $\mathcal{S}_2$ se quieran. Por otra parte, la Proposición 3.5 hace lo mismo con $\mathcal{S}_3$ pero en principio no queda claro cómo generar sus números de forma eficiente debido a las restricciones para las variables x, y, z. La teoría clásica sobre representaciones de formas cuadráticas ternarias tratadas por [**?**] permite obtener una parametrización en términos de ciertos grupos. Partiendo de:

$$\mathbf{SL}_2(\mathbb{Z}) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \,:\, a, b, c, d \in \mathbb{Z},\, ad - bc = 1 \right\},$$

se realiza la identificación de cada matriz A con su matriz opuesta $-A$ obteniendo el grupo:

$$\mathbf{PSL}_2(\mathbb{Z}) := \mathbf{SL}_2(\mathbb{Z})/\{\pm \mathrm{Id}\}.$$

Por otra parte, se considera:

$$\Gamma_0(2) := \left\{ A \in \mathbf{SL}_2(\mathbb{Z}) \,:\, A \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \pmod 2 \right\}.$$

El estudio de formas cuadráticas ternarias puede reducirse al de las formas cuadráticas binarias $AX^2+2BXY+CY^2$, las cuales pueden representarse mediante el vector (A, B, C), su *determinante* viene dado por $D = B^2 - AC$ y su *discriminante* es $\Delta = 4D$ (ambos pueden ser vistos como una forma ternaria en A, B y C). En el conjunto de todas las formas cuadráticas binarias de cierto determinante D, es posible establecer una relación de equivalencia. Más concretamente, se dirá que (A, B, C) es *equivalente* a (A', B', C') si existen $(\alpha, \beta, \gamma, \delta)$ enteros tales que $\alpha\delta - \beta\gamma = 1$ y una forma se transforma en la otra a través del cambio $X' = \alpha X + \beta Y$, $Y' = \gamma X + \delta Y$, es decir:

$$A' = A\alpha^2 + 2B\alpha\gamma + C\gamma^2, \quad B' = A\alpha\beta + B(\alpha\delta + \beta\gamma) + C\gamma\delta, \quad C' = A\beta^2 + 2B\beta\delta + C\delta^2.$$

El número de clases de equivalencia, llamado simplemente *número de clases*, depende de D de una manera en general bastante desconocida y ligada a la factorización en ideales. Sin embargo, en el caso en que $D = d^2$ con d positivo es muy sencillo calcularlo, dando incluso las clases de equivalencia de forma explícita:

Lema 3.10 (Gauss) *Toda forma cuadrática binaria de determinante d^2 es equivalente a una de las formas $AX^2 + 2dXY$, con $A = 0, \ldots, 2d-1$, siendo estas no equivalentes entre sí.*

Demostración. Al ser $d^2 = B^2 - AC$, se tiene $(d-B)/A = -C/(d+B)$. Sea β/δ esta razón expresada en forma irreducible. Entonces por la *identidad de Bézout* es posible hallar α y γ tales que $\alpha\delta - \beta\gamma = 1$. De esta manera, si (A', B', C') es equivalente a (A, B, C), al desarrollar los coeficientes de (A', B', C') en función de los de (A, B, C), se obtiene en particular:

$$B' = A\alpha\beta + B(\alpha\delta + \beta\gamma) + C\gamma\delta = (d-B)\alpha\delta + B(\alpha\delta + \beta\gamma) - (d+B)\beta\gamma = d(\alpha\delta - \beta\gamma) = d,$$

$$C' = A\beta^2 + 2B\beta\delta + C\delta^2 = (d-B)\beta\delta + 2B\beta\delta - (d+B)\beta\delta = 0.$$

Si al hacer la sustitución, A' es uno de los números entre 0 y $2d-1$, entonces (A', B', C') satisface todas las condiciones requeridas. Por otra parte, si A' no fuese ninguno de dichos números, sea A'' el residuo positivo mínimo de A' módulo $2d$, de manera que $A'' - A' = 2dm$. Entonces mediante la transformación $(1, 0, m, 1)$ la forma $(A', B', C') = (A', d, 0)$ será equivalente a $(A'', d, 0)$ y esta satisfará las condiciones requeridas. Además, la forma (A, B, C) puede transformarse mediante $(\alpha + \beta m, \beta, \gamma + dm, \delta)$ en $(A'', d, 0)$. Por último, si $(A, d, 0)$ y $(A', d, 0)$ no son idénticas (es decir, $A \neq A'$), entonces no pueden ser equivalentes. Si lo fueran, la primera se transformaría mediante ciertos $(\alpha, \beta, \gamma, \delta)$ en la segunda. Al hacerlo, se obtendrían las ecuaciones:

$$A\alpha^2 + 2d\alpha\gamma = A', \quad A\alpha\beta + d(\alpha\delta + \beta\gamma) = d, \quad A\beta^2 + 2d\beta\delta = 0, \quad \alpha\delta - \beta\gamma = 1.$$

Al multiplicar la segunda ecuación por β, la tercera por α, restar ambas y usar la cuarta se llega a que necesariamente $\beta = 0$ y de ahí que $\alpha\delta = 1$. Así, $\alpha = \pm 1$ y empleando la primera ecuación se deduce que $A \pm 2\gamma d = A'$. Ya que tanto A como A' están entre 0 y $2d-1$, esta ecuación no es consistente a menos que $\gamma = 0$, es decir, a menos que $A = A'$. De ahí se concluye que ambas formas deben ser idénticas. □

En el caso de la ecuación $x^2 + y^2 - z^2 = 1$, pueden aplicarse formas cuadráticas para conseguir el siguiente resultado:

Proposicion 3.11 *Sean el grupo y el cogrupo a la izquierda:*

$$\Gamma_0 := \mathbf{PSL}_2(\mathbb{Z}), \qquad \Gamma_1 := \begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix} \Gamma_0(2)/\{\pm \mathrm{Id}\},$$

y sean las aplicaciones $T_j : \Gamma_j \longrightarrow \mathbb{Z}^3$ para $j = 0,\ 1$ dadas por:

$$T_j(g) = \left(cd - ab + \frac{1}{2}j(c^2 - a^2), -ad - bc - jac, ab + cd + \frac{1}{2}j(a^2 + c^2) \right) \quad con \quad g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Entonces T_0 y T_1 son inyectivas y $T_0(\Gamma_0) \cup T_1(\Gamma_1)$ es una partición del conjunto de soluciones enteras de la ecuación $x^2 + y^2 - z^2 = 1$.

Demostración. Dado que el discriminante de una forma cuadrática $\Delta(A, B, C) = 4(B^2 - AC)$ puede verse como una forma cuadrática ternaria, para $\vec{w} = (x, y, z)$ se cumple:

$$\Delta(M\vec{w}) = 4(x^2 + y^2 - z^2) \quad \text{con} \quad M = \begin{pmatrix} -1 & 0 & 1 \\ 0 & -1 & 0 \\ 1 & 0 & 1 \end{pmatrix}.$$

Entonces la condición $x^2 + y^2 - z^2 = 1$ se traduce en que la forma cuadrática binaria correspondiente a $M\vec{w}$ tiene discriminante $4 = 4 \cdot 1^2$, por lo que por el Lema 3.10, es equivalente a $2XY$ o a $X^2 + 2XY$, que pueden asociarse a los vectores $\vec{c_0} = (0, 1, 0)$ y $\vec{c_1} = (1, 1, 0)$ respectivamente. La equivalencia de formas binarias, como se ha visto, corresponde en términos de sus matrices A 2×2 a la asociación $A \sim gAg^t$, con $g \in \Gamma_0$. Asimismo, en términos de los vectores tridimensionales, esta asociación corresponde a la representación $R : \Gamma_0 \longrightarrow \mathrm{GL}_3$ dada por:

$$R(g) = \begin{pmatrix} a^2 & 2ab & b^2 \\ ac & ad + bc & bd \\ c^2 & 2cd & d^2 \end{pmatrix} \quad \text{para} \quad g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0.$$

Entonces cada solución $\vec{w} = (x, y, z) \in \mathbb{Z}^3$ de la ecuación $x^2 + y^2 - z^2 = 1$ satisface o bien $M\vec{w} = R(g)\vec{c_0}$ o bien $M\vec{w} = R(g)\vec{c_1}$ para alguna matriz $g \in \Gamma_0$ y ambas posibilidades no pueden ocurrir simultáneamente ya que por el Lema 3.10 las formas $2XY$ y $X^2 + 2XY$ no son equivalentes. En consecuencia, el conjunto de soluciones viene dado por la partición:

$$\bigcup_{j=0}^{1} \left\{ M^{-1}R(g)\vec{c_j} : g \in \Gamma_0 \right\} \cap \mathbb{Z}^3.$$

Además, para $j = 0, 1$ se cumple que $M^{-1}R(g)\vec{c_j} = T_j(g)$. Por tanto, dado el aspecto de las fórmulas de T_j del enunciado, directamente $M^{-1}R(\Gamma_0)\vec{c_0} \subset \mathbb{Z}^3$ y para que se verifique $M^{-1}R(g)\vec{c_1} \in \mathbb{Z}^3$ es necesario y suficiente que la primera columna de g tenga entradas impares, es decir, $g \in \Gamma_1$, ya que todo elemento de Γ_1 se expresa como:

$$\begin{pmatrix} a + c & b + d \\ -a & -b \end{pmatrix}, \quad \text{con} \quad ad - bc = 1, \quad 2 \mid c;$$

por lo que la primera columna tiene forzosamente entradas impares (si no lo fueran, entonces $2 \mid a$, lo que contradiría que $ad - bc = 1$). □

A la hora de obtener computacionalmente las tuplas (x, y, z) verificando $x^2 + y^2 - 1 = z^2$, en principio no está claro cómo restringir los parámetros a, b, c y d para obtener todas las soluciones con x^2, y^2, $z^2 \leq N$ de forma efectiva. Acotando como primera idea el tamaño de las entradas a, b, c y d en las matrices y tratando en un rango amplio las parametrizaciones dadas por la Proposición 3.11, esta estrategia no resulta adecuada ya que las mismas dejan fuera muchas de las soluciones fijado un N. Esto es debido a que en muchos casos (y con más frecuencia

conforme el tamaño de las entradas se va acercando a N) alguna de las entradas es mucho mayor en comparación al resto y eso hace que la solución correspondiente quede fuera. Para solucionar este problema se puede proceder de la siguiente forma. Quitando las soluciones triviales se tiene $z^2 = \max\{x^2, y^2, z^2\}$. Por tanto, interesa imponer como punto de partida $z^2 \leq N$. De las dos parametrizaciones diferentes provenientes de la Proposición 3.11:

$$\begin{cases} x = -ab + cd, \\ y = -ad - bc, \\ z = ab + cd; \end{cases} \qquad \begin{cases} x = \frac{1}{2}\left(b^2 + c^2 - a^2 - d^2\right), \\ y = bd - ac, \\ z = \frac{1}{2}\left(a^2 + c^2 - b^2 - d^2\right); \end{cases}$$

como $1 = (ad - bc)^2 = a^2d^2 + b^2c^2 - 2abcd$, para la primera parametrización se tiene:

$$z^2 = (ab + cd)^2 = a^2d^2 + b^2c^2 + 2abcd = a^2b^2 + c^2d^2 + a^2d^2 + b^2c^2 - 1 = (a^2 + c^2)(b^2 + d^2) - 1.$$

Por tanto, obtener todas las soluciones con x^2, y^2, $z^2 \leq N$ correspondientes a la primera parametrización es sinónimo de recorrer los parámetros a, b, c y d tales que $(a^2 + c^2)(b^2 + d^2) \leq N + 1$. Para reducir el número de operaciones es posible aprovechar la simetría que existe entre (a, c) y (b, d) y realizar un bucle en la computadora que recorra solo a y c con $a^2 + c^2 \leq \sqrt{N+1}$ y posteriormente para cada a y c hallar todos los b y d a través de la *Identidad de Bézout* $ad - bc = 1$ tales que $b^2 + d^2 \leq (N + 1)/(a^2 + c^2)$. En cuanto a la segunda parametrización, está relacionada con la primera gracias al cambio:

$$a \mapsto \frac{a - b}{\sqrt{2}}, \qquad b \mapsto \frac{a + b}{\sqrt{2}}, \qquad c \mapsto \frac{c - d}{\sqrt{2}}, \qquad d \mapsto \frac{c + d}{\sqrt{2}}.$$

Repitiendo el mismo argumento anterior con z^2 pero a través de este cambio se llega a:

$$z^2 = \frac{1}{4}\left(\tilde{a}^2 + \tilde{c}^2\right)\left(\tilde{b}^2 + \tilde{d}^2\right) - 1 \qquad \text{con} \quad \tilde{a}\tilde{d} - \tilde{b}\tilde{c} = 2,$$

donde $\tilde{a} = a - b$, $\tilde{b} = c - d$, $\tilde{c} = a + b$, $\tilde{d} = c + d$. De esta forma, el bucle que habría que recorrer es el mismo pero cambiando en la *Identidad de Bézout* un 1 por un 2.

B. Caracterización de $\mathcal{S}_4$. La estructura de $\mathcal{S}_4$ es algo más complicada y para precisarla se parte del siguiente planteamiento. Al observar las ecuaciones $(K4)$, y más concretamente las formas cuadráticas x^2+y^2 y $x^2+4xy+y^2$ del primer miembro de cada una de ellas, la primera se distingue por ser más simple (diagonal) y tener mayor número de simetrías, mientras que en la segunda así como en el resto de ecuaciones para el resto de los $\mathcal{S}_K$ con $K \geq 4$ se incluye un término extra en xy. Sin embargo, es posible diagonalizar simultáneamente todas las formas sobre $\mathbb{Q}$, adquiriendo de esta manera un aspecto más simple y uniforme. En el caso de $\mathcal{S}_4$, para cada x, $y \in \mathbb{Z}$ existen unos únicos X, $Y \in \mathbb{Z}$ con $X \equiv Y \pmod 2$ tales que $x = (X + Y)/2$ e $y = (Y - X)/2$. Al sustituir en las ecuaciones de $(K4)$ se obtiene:

$$X^2 + Y^2 = 2 + 2z_0^2, \qquad X^2 - 3Y^2 = 6 - 2z_1^2.$$

Manipulando las ecuaciones tomando $a = z_0 - Y$, $b = z_0 + Y$, $c = X - z_1$ y $d = X + z_1$ se concluye:

$$3ab = cd, \qquad c^2 + d^2 - a^2 - b^2 = 8,$$

considerando además las condiciones de divisibilidad $2 \mid a - b$, $2 \mid c - d$ y $4 \mid b - a + c + d$. Estas condiciones vienen garantizadas para poder pasar del primer grupo de ecuaciones al segundo, ya que si $2 \nmid a - b$ o $2 \nmid c - d$, entonces no se podría despejar la Y o la X en los cambios tomados, y si $4 \nmid b - a + c + d$, entonces $4 \nmid 2(X + Y)$, lo cual contradice que X e Y se hayan considerado con la misma paridad. Esta reformulación presenta la ventaja de la manejabilidad de las ecuaciones resultantes, especialmente la primera de ellas, y su conjunto de soluciones se corresponde con el conjunto de soluciones de $(K4)$.

Una vez que se ha realizado la diagonalización simultánea, la idea que se sigue es que para cualquier m las soluciones de $c^2 + d^2 - a^2 - b^2 = m$ pueden parametrizarse sin obviar ninguna a través de $\mathbf{SL}_2(\mathbb{Z})$ **[?]**. Más concretamente, la forma cuadrática $x_1x_4 - x_2x_3$ (que se asemeja al determinante de una matriz 2×2) se diagonaliza como $y_1^2+y_2^2-y_3^2-y_4^2$. De esta forma, las soluciones de $(K4)$ vienen dadas por matrices de $\mathbf{SL}_2(\mathbb{Z})$ que satisfacen una condición de divisibilidad extra (correspondiente a la primera ecuación resultante de la diagonalización simultánea). Esta condición permitirá construir una llamada *ecuación de Pell generalizada*. De esta forma se establecerá una correspondencia biyectiva entre las soluciones de $(K4)$ y las soluciones de las ecuaciones de Pell generalizadas obtenidas tras la elección de cada racional posible. Sin embargo, no se utilizará $\mathbf{SL}_2(\mathbb{Z})$ en sí para establecer la

biyección, ya que aparecerán denominadores que solo podrán ser simplificados para cierto subconjunto del conjunto Γ_2 de matrices 2×2 enteras de determinante 2, si bien este último se puede interpretar como 3 copias de $\mathbf{SL}_2(\mathbb{Z})$, concretamente:

$$\Gamma_2=\bigcup_{k=0}^{2}\mathcal{G}_k,\qquad \mathcal{G}_k=\mathbf{SL}_2(\mathbb{Z})\mathfrak{g}_k,\quad \mathfrak{g}_0=\begin{pmatrix}2&0\\0&1\end{pmatrix},\quad \mathfrak{g}_1=\begin{pmatrix}1&1\\0&2\end{pmatrix},\quad \mathfrak{g}_2=\begin{pmatrix}1&0\\0&2\end{pmatrix}.$$

Esta descomposición es una partición, es decir, los $\mathcal{G}_k$ son disjuntos entre sí.

Para poder formalizar todo el planteamiento anterior y describir la familia recién referida, se enuncia el siguiente resultado:

Teorema 3.12 *Sean las tuplas de enteros impares (λ,μ,u,v) que verifican la ecuación:*

$$\delta_0^2(9v^2-u^2)\lambda^2-(v^2-u^2)\mu^2=8\quad con\quad \delta_0=\begin{cases}1 & si\ 3\nmid u,\\ 1/3 & si\ 3\mid u.\end{cases}$$

Sea $\mathcal{M}$ el conjunto de tales tuplas módulo un cambio global de signo. Entonces las fórmulas:

$$\begin{cases} x=\dfrac{1}{4}\left(\mu(u+v)+\delta_0\lambda(u-3v)\right), & y=\dfrac{1}{4}\left(\mu(v-u)+\delta_0\lambda(u+3v)\right),\\[2ex] z_0=\dfrac{1}{2}\left(\mu v-\delta_0\lambda u\right), & z_1=\dfrac{1}{2}\left(\mu u+3\delta_0\lambda v\right)\end{cases}$$

establecen una biyección entre $\mathcal{M}$ y el conjunto de soluciones enteras de $(K4)$.

Demostración. Se considera el conjunto de matrices de determinante 2:

$$\mathcal{H}=\left\{\begin{pmatrix}\alpha&\beta\\\gamma&\delta\end{pmatrix}\in\mathcal{G}_1:3(\beta+\gamma)(\delta-\alpha)=(\beta-\gamma)(\delta+\alpha)\right\}.$$

Toda matriz de $\mathcal{G}_1$ es de la forma:

$$\begin{pmatrix}a&a+2c\\c&c+2d\end{pmatrix}\quad\text{con}\quad\begin{pmatrix}a&b\\c&d\end{pmatrix}\in\mathbf{SL}_2(\mathbb{Z}).$$

Por tanto $2\mid\alpha-\beta$, $2\mid\gamma-\delta$ y α y γ no pueden ser ambos pares. De hecho esta última propiedad junto con la condición $\alpha\delta-\beta\gamma=2$ determina $\mathcal{G}_1$. Sea ahora la aplicación:

$$\Phi(x,y,z_0,z_1)=\frac{1}{2}\begin{pmatrix}z_1-z_0-2y&z_0-z_1-2y\\z_0+z_1-2x&z_0+z_1+2x\end{pmatrix},$$

cuyo determinante es $-2xy+(z_1^2-z_0^2)/2$ y vale 2 para toda tupla (x,y,z_0,z_1) solución de $(K4)$. Si además (x,y,z_0,z_1) es una tupla de enteros entonces $2\mid z_1-z_0$ y $\Phi(x,y,z_0,z_1)\mathfrak{g}_1^{-1}$ tiene entradas enteras y determinante 1. Con esto se llega a que Φ es una aplicación del conjunto de soluciones enteras de $(K4)$ en $\mathcal{G}_1$. En realidad, $\mathrm{im}(\Phi)\subseteq\mathcal{H}$, ya que todo elemento de $\mathrm{im}(\Phi)$ verifica, imponiendo la condición de $\mathcal{H}$, la ecuación $3(z_0-x-y)(z_0+x+y)=(-z_1+x-y)(z_1+x-y)$, es decir, $4x^2+4xy+4y^2=3z_0^2+z_1^2$, que es una combinación lineal de las ecuaciones de $(K4)$. Por otra parte, sea en $\mathcal{H}$ la aplicación:

$$\Psi\begin{pmatrix}\alpha&\beta\\\gamma&\delta\end{pmatrix}=\left(\frac{\delta-\gamma}{2},-\frac{\alpha+\beta}{2},\frac{-\alpha+\beta+\gamma+\delta}{2},\frac{\alpha-\beta+\gamma+\delta}{2}\right).$$

Se cumple $\mathrm{im}(\Psi)\subseteq\mathbb{Z}^4$ ya que $2\mid\alpha-\beta$ y $2\mid\gamma-\delta$. Además, $(\Psi\circ\Phi)(x,y,z_0,z_1)=(x,y,z_0,z_1)$, por lo que Φ y Ψ son inversas y así Φ establece una biyección entre el conjunto de soluciones enteras de $(K4)$ y $\mathcal{H}$. A continuación, se procede a precisar el aspecto de los elementos de $\mathcal{H}$. Sea $\mu=\mathrm{mcd}(\alpha,\delta)$. Entonces ambos parámetros pueden expresarse como $\alpha=\mu(u-v)/2$, $\delta=\mu(u+v)/2$ para ciertos u y v tales que $2\mid u-v$. Si se excluye el caso $\alpha=\delta=0$, una vez que se especifica el signo de $\mathrm{mcd}(\alpha,\delta)$, los valores de μ, u y v quedan totalmente determinados y sustituyendo las fórmulas de α y δ en la condición de $\mathcal{H}$, se obtiene $\beta(3v-u)=\gamma(u+3v)$. Puesto que $(u-v)/2$ y $(u+v)/2$ son coprimos, para $3\nmid u$:

$$\begin{aligned}\mathrm{mcd}\left(\frac{u+3v}{2},\frac{3v-u}{2}\right)&=\mathrm{mcd}\left(\frac{u+3v}{2},2\cdot\frac{u+3v}{2}-\frac{3v-u}{2}\right)=\mathrm{mcd}\left(3\cdot\frac{u+v}{2},\frac{u+3v}{2}\right)\\&=\mathrm{mcd}\left(\frac{u+v}{2},\frac{u+3v}{2}\right)=\mathrm{mcd}\left(\frac{u+v}{2},2\cdot\frac{u+v}{2}-\frac{u+3v}{2}\right)=\mathrm{mcd}\left(\frac{u+v}{2},\frac{u-v}{2}\right)=1,\end{aligned}$$

mientras que para $3 \mid u$:

$$\begin{aligned}\operatorname{mcd}\left(\frac{u+3v}{2}, \frac{3v-u}{2}\right) &= 3 \cdot \operatorname{mcd}\left(\frac{u+3v}{6}, \frac{3v-u}{6}\right) = 3 \cdot \operatorname{mcd}\left(2 \cdot \frac{u+3v}{6} - \frac{3v-u}{6}, \frac{3v-u}{6}\right) \\ &= 3 \cdot \operatorname{mcd}\left(\frac{u+v}{2}, \frac{3v-u}{6}\right) = 3 \cdot \operatorname{mcd}\left(\frac{u+v}{2}, \frac{1}{2} \cdot \frac{u+v}{2} - \frac{3}{2} \cdot \frac{3v-u}{6}\right) = 3 \cdot \operatorname{mcd}\left(\frac{u+v}{2}, \frac{u-v}{2}\right) = 3.\end{aligned}$$

Por tanto, $\operatorname{mcd}\left((u+3v)/2, (3v-u)/2\right) = \delta_0^{-1}$. Escribiendo $\lambda = \operatorname{mcd}(\beta, \gamma)$, se puede deducir que $\beta = -\delta_0\lambda(u+3v)/2$ y $\gamma = -\delta_0\lambda(u-3v)/2$. El caso $\beta = \gamma = 0$ no tiene por qué excluirse si se toma $\operatorname{mcd}(0,0) = 0$ por convenio, ya que $(u+3v)/2$ y $(u-3v)/2$ no son ambos cero (si lo fueran, entonces $u = v = 0$ y se tendría $\alpha = \delta = 0$). De igual forma, en el caso $\alpha = \delta = 0$ se puede tomar $\mu = 0$ y utilizar las expresiones de β y γ para definir u y v. En resumen, se ha probado:

$$\mathcal{H} = \left\{ \frac{1}{2} \begin{pmatrix} \mu(u-v) & -\delta_0\lambda(u+3v) \\ -\delta_0\lambda(u-3v) & \mu(u+v) \end{pmatrix} \in \mathcal{G}_1 \,:\, \operatorname{mcd}\left(\frac{u+v}{2}, \frac{u-v}{2}\right) = 1 \right\}.$$

Siguiendo en la línea de simplificar la caracterización de $\mathcal{H}$, si $2 \mid \mu$, entonces $2 \mid \alpha, \delta$. Como las condiciones de paridad exigidas en $\mathcal{G}_1$ aseguran que $2 \mid \gamma - \delta$ y α y γ no son ambos pares, se llega a contradicción. De forma análoga, si $2 \mid \lambda$, entonces $2 \mid \beta, \gamma$. En este caso, como las condiciones de paridad aseguran que $2 \mid \alpha - \beta$ y α y γ no son ambos pares, también se llega a contradicción. Por último, si $2 \mid u$ o $2 \mid v$, en realidad ambos serían pares (ya que fueron tomados desde el principio tales que $2 \mid u - v$). Esto implica que el determinante de la matriz correspondiente en $\mathcal{H}$ sería múltiplo de 4 y por tanto no podría ser 2. Además, la propia condición del determinante implica que $u+v$ y $u-v$ no puedan tener divisores impares comunes. En conclusión, la caracterización de $\mathcal{H}$ quedaría:

$$\mathcal{H} = \left\{ \frac{1}{2} \begin{pmatrix} \mu(u-v) & -\delta_0\lambda(u+3v) \\ -\delta_0\lambda(u-3v) & \mu(u+v) \end{pmatrix} \text{ con determinante 2 y } 2 \nmid \lambda, \mu, u, v \right\}.$$

Para finalizar, los parámetros λ, μ, u y v quedan completamente determinados por la matriz salvo por un cambio de signo en $(\lambda, \mu) = (\operatorname{mcd}(\beta, \gamma), \operatorname{mcd}(\alpha, \delta))$, lo cual está relacionado con el correspondiente cambio de signo de u y v. Imponiendo que el determinante sea 2 se obtiene la ecuación del enunciado y al aplicar Ψ se concluyen las fórmulas respectivas para x, y, z_0 y z_1. □

La dependencia de x e y con respecto al factor δ_0 puede simplificarse en cierta forma, aunque la consecuencia de esta acción sería perder una biyección perfecta, debido a que se permitiría cierta incertidumbre en los signos de z_0 y z_1:

Corolario 3.13 *Para cada solución $(\lambda, \mu, u, v) \in \mathbb{Z}^4$ de la ecuación:*

$$(P) \qquad 9v^2\lambda^2 - u^2\lambda^2 - v^2\mu^2 + u^2\mu^2 = 8, \qquad \textit{con} \quad u \equiv v \equiv \lambda \equiv \mu \equiv 1 \,(\operatorname{mod} 2),$$

se obtiene una solución entera de $(K4)$ dada por:

$$x = \frac{1}{4}\left(\mu(u+v) + \lambda(u-3v)\right), \qquad y = \frac{1}{4}\left(\mu(v-u) + \lambda(u+3v)\right).$$

Recíprocamente, cada solución entera de $(K4)$ da una solución entera de (P).

Demostración. Si $3 \nmid u$, las fórmulas para x e y vienen dadas directamente por el Teorema 3.12. Si $3 \mid u$, cambiando (λ, μ, u, v) por $(-\mu, \lambda, -v, u/3)$, se sigue satisfaciendo la ecuación (P) y puesto que u y v son necesariamente coprimos (si no lo fueran, observando (P) se deduciría que 8 tendría un divisor impar, lo cual es falso), se sigue que $3 \nmid v$. Recíprocamente, al sustituir directamente las fórmulas para x, y, z_0 y z_1 dadas por el Teorema 3.12 tomando $\delta_0 = 1$ se muestra que satisfacen $(K4)$. □

Recuperando la biyección Φ establecida en el Teorema 3.12, su utilidad va mucho más allá de la vista en la demostración del resultado y posteriores consecuencias. Tal y como se ha estudiado en la Proposición 3.8, tomando únicamente la primera ecuación de $(K4)$, se puede observar cómo posee 16 simetrías generadas por los cambios de signo $x \leftrightarrow -x$, $y \leftrightarrow -y$, $z \leftrightarrow -z$ y la permutación $x \leftrightarrow y$. Sin embargo, para la segunda ecuación de $(K4)$, los cambios de signo $(x, y) \leftrightarrow (x, -y)$, $(x, y) \leftrightarrow (-x, y)$ no son posibles, por lo que las simetrías se reducen a 8, generadas por $(x, y) \leftrightarrow (-x, -y)$, $z \leftrightarrow -z$ y $x \leftrightarrow y$. Hasta ahí, parece que no hay más que decir acerca de las simetrías, pero teniendo en cuenta que en cada ecuación los z correspondientes son distintos, al introducir la biyección Φ surgen

nuevas simetrías ocultas con las que se obtiene un grupo de 32 elementos no conmutativo. Tomando una matriz de $\mathcal{H}$ como en la demostración del Teorema 3.12, la condición impuesta $3(\beta+\gamma)(\delta-\alpha)=(\beta-\gamma)(\alpha+\delta)$ queda invariante por los cambios $(\alpha,\delta)\mapsto(-\alpha,-\delta)$ y $(\beta,\gamma)\mapsto(-\beta,-\gamma)$. En particular, el cambio $(\alpha,\beta,\gamma,\delta)\mapsto(-\alpha,\beta,\gamma,-\delta)$ tiene como matriz $s_5=\mathrm{diag}(-1,1,1,-1)^t$ y si A es la matriz de la aplicación lineal dada por Ψ en la demostración del Teorema 3.12:

$$A=\begin{pmatrix} 0 & 0 & -1/2 & 1/2 \\ -1/2 & -1/2 & 0 & 0 \\ -1/2 & 1/2 & 1/2 & 1/2 \\ 1/2 & -1/2 & 1/2 & 1/2 \end{pmatrix},$$

entonces la aplicación $\vec{x}\mapsto As_5A^{-1}\vec{x}$ lleva soluciones de $(K4)$ a soluciones de $(K4)$ necesariamente. Haciendo los cálculos, la matriz As_1A^{-1} no es más que la matriz correspondiente a la simetría L_5 de la Proposición 3.8. El otro cambio $(\alpha,\beta,\gamma,\delta)\mapsto(\alpha,-\beta,-\gamma,\delta)$ origina la misma matriz de L_5 con un signo $-$ global. Por tanto, la biyección Φ revela la simetría L_5, que no siendo observable directamente a partir de las ecuaciones de $(K4)$, se convierte en trivial vista desde $\mathcal{H}$. Haciendo lo mismo con el resto de simetrías L_i para $1\leq i\leq 4$, cada matriz As_iA^{-1} actúa sobre un elemento de $\mathcal{H}$ pasándolo respectivamente a:

$$\frac{1}{2}\begin{pmatrix} \alpha-\beta+\gamma-\delta & -\alpha+\beta+\gamma-\delta \\ \alpha+\beta+\gamma+\delta & -\alpha-\beta+\gamma+\delta \end{pmatrix},\qquad \begin{pmatrix} -\beta & \alpha \\ \delta & \gamma \end{pmatrix},\qquad \begin{pmatrix} \gamma & -\delta \\ \alpha & -\beta \end{pmatrix},\qquad \begin{pmatrix} -\delta & \gamma \\ \beta & -\alpha \end{pmatrix}.$$

En este sentido, simetrías como L_1, que son triviales vistas en las ecuaciones de $(K4)$, se vuelven oscuras vistas desde $\mathcal{H}$.

C. Ecuaciones de Pell generalizadas. Sea la llamada *ecuación de Pell generalizada* $AX^2-BY^2=1$. A priori, se puede decir que para que esta ecuación tenga solución no trivial claramente A y B deben ser coprimos y del mismo signo. Considerando sin pérdida de generalidad A, $B>0$ [3] tales que AB no es un cuadrado perfecto (para evitar casos triviales[4]), no se conocen a ciencia cierta condiciones sencillas para decidir la existencia de soluciones, aunque es cierto que si existe una, entonces existen infinitas y las que son positivas vienen dadas por la fórmula [**?**]:

$$X\sqrt{A}+Y\sqrt{B}=\left(x_0\sqrt{A}+y_0\sqrt{B}\right)^{2n-1},\qquad n\in\mathbb{Z}^+;$$

donde (x_0,y_0) es una solución positiva particular con x_0 e y_0 mínimos llamada *solución fundamental*. Incorporando a esta fórmula un $\pm$ en el segundo miembro y permitiendo $n\in\mathbb{Z}$ se obtienen todas las soluciones enteras de la ecuación, positivas y negativas. El problema de la existencia de soluciones de la ecuación y del tamaño de las soluciones fundamentales puede ser atacado de forma computacional, ya que existen algoritmos basados en fracciones continuas [**?**] y otros en métodos más sofisticados [**?**] para encontrar la solución fundamental o decidir que no existe.

Aplicado a la caracterización de $\mathcal{S}_4$ dada por el Teorema 3.12, dados u y v impares, se construye la ecuación:

$$A\lambda^2-B\mu^2=1,\qquad A:=\delta_0^2\frac{9v^2-u^2}{8},\quad B:=\frac{v^2-u^2}{8}.$$

Al ser u y v impares, se cumple que A, $B\in\mathbb{Z}$. Por tanto, para hallar todas las soluciones de $(K4)$ basta considerar un racional adecuado u/v, construir su correspondiente ecuación de Pell generalizada y calcular sus soluciones (λ,μ) en el caso de que existan. Para las primeras soluciones de $(K4)$ se tienen las siguientes tuplas:

x	y	λ	μ	u	v
19	13	3	5	9	11
65	26	3	7	21	23
69	53	7	11	15	19
127	76	5	27	11	13
151	43	1	9	37	39

x	y	λ	μ	u	v
188	129	1	5	89	109
206	127	13	23	21	25
274	127	9	19	33	37
289	64	3	11	57	59
404	321	11	17	57	73

Al observar tal disparidad en las elecciones de los racionales u/v (o λ/μ, ya que la ecuación es simétrica según el cambio $(\lambda,\mu)\leftrightarrow(u,v)$), surge la duda acerca de cómo recorrer tal infinidad de racionales u/v de una forma

[3] Si A, $B<0$, basta cambiar (A,X,B,Y) por $(-B,Y,-A,X)$, obteniendo una nueva ecuación de Pell generalizada cuyos coeficientes son positivos.

[4] Si $AB=D^2$ entonces $AX^2-BY^2=A^{-1}(AX-DY)(AX+DY)$ y obviamente solo hay un número finito de soluciones entras de $AX^2-BY^2=1$.

que resulte eficiente o bien pensar en si los racionales que se deben escoger están limitados por alguna condición. Apelando a las fórmulas para x, y, z_0 y z_1 dadas en el Teorema 3.12 es posible delimitar el rango de recorrido de u/v de la siguiente forma:

Lema 3.14 *Si la tupla (x, y, z_0, z_1) es solución de $(K4)$ con $x > y > 0$ y $z_0, z_1 > 0$, entonces λ, μ, u, $v > 0$ y $u/v \in (2\sqrt{3} - 3, 1)$.*

Demostración. La ecuación $A\lambda^2 - B\mu^2 = 1$ tendrá solución únicamente si A y B tienen el mismo signo, es decir, si $\operatorname{sgn}(9v^2 - u^2) = \operatorname{sgn}(v^2 - u^2)$. Imponiendo esta condición se concluye que necesariamente $u/v \in (-\infty, -3) \cup (-1, 1) \cup (3, +\infty)$. Suponiendo sin pérdida de generalidad que $u + v > 0$,[5] al tomar las fórmulas para x, y, z_0 y z_1 en función de λ, μ, u y v dadas por el Teorema 3.12 y teniendo en cuenta que si $x > y > 0$ entonces $z_1 > z_0$, se pueden establecer las siguientes equivalencias:

$$\begin{cases} x > 0 & \Leftrightarrow & \mu(u+v) + \delta_0\lambda(u-3v) > 0, \\ y > 0 & \Leftrightarrow & \mu(v-u) + \delta_0\lambda(u+3v) > 0, \\ z_0 > 0 & \Leftrightarrow & \mu v - \delta_0\lambda u > 0, \\ z_1 > 0 & \Leftrightarrow & \mu u + 3\delta_0\lambda v > 0, \\ x > y & \Leftrightarrow & \mu u - 3\delta_0\lambda v > 0, \\ z_1 > z_0 & \Leftrightarrow & \mu(u-v) + \delta_0\lambda(u+3v) > 0. \end{cases}$$

Antes de proceder, el caso $v = 0$ es imposible, porque implicaría por la cuarta o quinta inecuaciones que $\mu > 0$ y por la tercera que $\lambda < 0$, pero esto contradice por la segunda inecuación que $-\mu u + \delta_0\lambda u > 0$, ya que para que $u+v > 0$ sea positivo, forzosamente $u > 0$ si se toma $v = 0$. De la misma manera, considerar $u+v = 0$ también lleva a contradicción, ya que de la primera inecuación se deduciría que λ y u son o ambos positivos o ambos negativos y recurriendo a la tercera o a la cuarta inecuaciones respectivamente, forzosamente sería $\mu < 0$ y ello produciría contradicción en la otra inecuación. Pasando ya a estudiar el sistema con $v \neq 0$, sumando la primera, tercera y cuarta inecuaciones se deduce que $\mu > 0$. Por otra parte, sumando la cuarta y quinta inecuaciones se obtiene $u > 0$, mientras que multiplicando por 2 la tercera inecuación y sumándole la primera y segunda se llega a que $v > 0$. Por tanto, el cociente u/v siempre es positivo. Además, en los casos $u - v > 0$ y $u - v < 0$, la segunda y la última inecuación implican respectivamente que $\lambda > 0$. Con esto se deduce que necesariamente $u/v \in (0, \infty)$ y que los parámetros λ, μ se pueden tomar positivos. Por último, manipulando un poco más las inecuaciones es posible reducir el rango para u/v. Despejando λ/μ de la quinta y sexta inecuaciones se establece la cadena:

$$\frac{v-u}{\delta_0(u+3v)} < \frac{\lambda}{\mu} < \frac{u}{3\delta_0 v}.$$

Eliminando λ/μ y operando se sigue $(u/v)^2 + 6u/v - 3 > 0$, lo cual implica que $u/v > 2\sqrt{3} - 3 \simeq 0,46410161513$ Con esto queda $u/v \in (2\sqrt{3} - 3, 1) \cup (3, \infty)$. Por último, para ver que u/v no puede estar en el segundo de los intervalos se despeja λ/μ de la segunda y quinta inecuaciones obteniendo:

$$\frac{u-v}{\delta_0(u+3v)} < \frac{\lambda}{\mu} < \frac{v}{\delta_0 u},$$

y eliminando de nuevo λ/μ se concluye que $u/v < 3$. □

Sobre el recíproco de este resultado se pueden precisar algunos aspectos. Fijado u/v proveniente del intervalo $(2\sqrt{3} - 3, 1)$, la ecuación $A\lambda^2 - B\mu^2 = 1$ tiene infinitas soluciones λ y μ. Si x e y son suficientemente grandes, entonces λ y μ también lo serán y al despejar λ/μ se obtendrá:

$$\left(\frac{\lambda}{\mu}\right)^2 = \frac{B}{A} + \frac{1}{A\mu^2} \sim \frac{B}{A} = \frac{v^2 - u^2}{\delta_0^2(9v^2 - u^2)}.$$

Para que esta cantidad sea comparable con la cota superior para λ/μ dada por la quinta inecuación de la prueba del Lema 3.14 debe cumplirse:

$$\frac{v^2 - u^2}{\delta_0^2(9v^2 - u^2)} < \frac{u^2}{9\delta_0^2 v},$$

[5] El Teorema 3.12 sostiene que existe una biyección salvo un cambio global de signo. Por tanto, cambiando la tupla (λ, μ, u, v) por $(-\lambda, -\mu, -u, -v)$ siempre se puede suponer $u + v > 0$.

es decir, $(u/v)^4 - 18(u/v)^2 + 9 < 0$. Atendiendo al rango del Lema 3.14, la única solución posible es $u/v > \sqrt{9-6\sqrt{2}} \simeq 0,7174389352\ldots$ Esto reduce el intervalo de partida de forma significativa para las soluciones suficientemente grandes. De hecho, el tener soluciones grandes es lo más plausible, ya que basta que B/A sea significativamente mayor que $(A\mu^2)^{-1}$, es decir, que B sea significativamente mayor que μ^{-2}. Al crecer μ, prácticamente la totalidad de los B cumplen el requisito, pudiendo tener excepciones para $v^2 - u^2$ suficientemente pequeño.

Para finalizar el análisis sobre la estructura de $\mathcal{S}_4$, a partir de la fórmula de las soluciones de la ecuación de Pell generalizada $AX^2 - BY^2 = 1$ referida al principio de este apartado, es posible obtener dos transformaciones que no modifican las soluciones de $(K4)$ dada una tupla (λ, μ, u, v):

Proposicion 3.15 *Las aplicaciones:*

$$(\lambda, \mu, u, v) \mapsto \left(\lambda + \frac{\lambda}{2}\mu^2(v^2 - u^2), -\mu + \frac{\mu}{2}\lambda^2(9v^2 - u^2), u, v\right),$$

$$(\lambda, \mu, u, v) \mapsto \left(\lambda, \mu, u + \frac{u}{2}v^2(\mu^2 - 9\lambda^2), -v + \frac{v}{2}u^2(\mu^2 - \lambda^2)\right)$$

actúan sobre (λ, μ, u, v) *preservando* (P).

Demostración. En general, si $AX^2 - BY^2 = 1$, entonces $(\sqrt{A}X + \sqrt{B}Y)(\sqrt{A}X - \sqrt{B}Y) = 1$. Al elevar esta identidad al cubo se obtiene $(\sqrt{A}X' + \sqrt{B}Y')(\sqrt{A}X' - \sqrt{B}Y') = 1$, es decir, $A(X')^2 - B(Y')^2 = 1$, donde $X' = AX^3 + 3BXY^2$, $Y' = BY^3 + 3AXY^2$. Por tanto, la transformación $X \mapsto X'$, $Y \mapsto Y'$ preserva soluciones de $AX^2 - BY^2 = 1$. Aplicándola al par (λ, μ), gracias a la ecuación (P) la transformación:

$$\lambda \mapsto \frac{9v^2 - u^2}{8}\lambda^3 + 3\frac{v^2 - u^2}{8}\lambda\mu^2 = \lambda + \frac{\lambda}{2}\mu^2(v^2 - u^2),$$

$$\mu \mapsto \frac{v^2 - u^2}{8}\mu^3 + 3\frac{9v^2 - u^2}{8}\lambda^2\mu = -\mu + \frac{\mu}{2}\lambda^2(9v^2 - u^2)$$

preserva soluciones de (P). De igual forma, dada la simetría $(\lambda, \mu) \leftrightarrow (u, v)$, lo anterior puede aplicarse a (u, v) y cambiando un signo irrelevante para la ecuación (P) se obtiene análogamente la otra transformación del enunciado.□

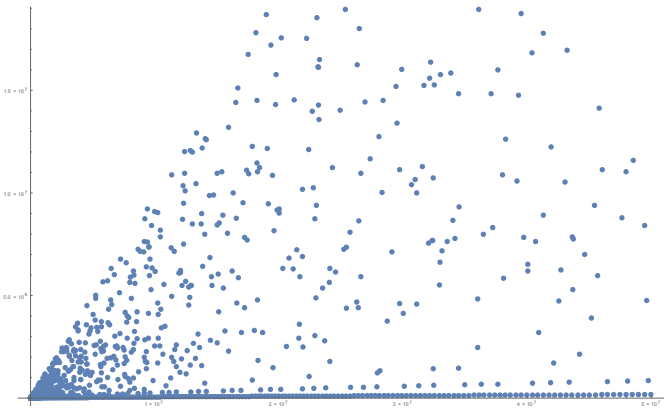
D. Familias polinómicas para $\mathcal{S}_4$. Si se aplica directamente el Corolario 3.13 a la tupla $(\lambda, \mu, u, v) = (1, 2k-1, 1, 1)$, únicamente se obtiene la familia de soluciones triviales de $(K4)$:

$$x(k) = k - 1, \qquad y(k) = 1.$$

Sin embargo, a través de la segunda transformación de la Proposición 3.15 se obtiene una nueva tupla $(\lambda, \mu, u, v) = (1, 2k-1, 2k^2 - 2k - 3, 2k^2 - 2k - 1)$, tal que al aplicar de nuevo el Corolario 3.13 la familia parametrizada por:

$$x(k) = 2k^3 - 4k^2 + 1, \qquad y(k) = 2k^2 - k - 2,$$

es solución no trivial de $(K4)$. Esta familia puede ser fácilmente observable directamente al computar los pares (x, y) soluciones no triviales de $(K4)$ cuyo tamaño no excede cierta cota. Por ejemplo, para $1 < y < x \leq 5 \cdot 10^7$, se obtiene una gráfica como la siguiente:



La familia anterior corresponde a la línea de puntos de la parte inferior de la gráfica, que casi parece continua. Una vez constatada, surge la duda de si esta es la única familia polinómica o existen otras más ocultas que no se aprecien tan fácilmente en la gráfica. La respuesta a este interrogante es afirmativa, y en realidad, esta primera familia que se ha encontrado será el caso $N = 1$ de una familia infinita de soluciones parametrizadas polinómicamente $(x_N(k), y_N(k))$ cuyo resto de miembros para $N > 1$, como se ha mencionado, no se detectan computacionalmente de forma tan sencilla. Para ello, es posible recurrir a una herramienta del *Análisis Numérico* [**?**]:

Definición 3.16 *La aproximante de Padé de orden $[n/n]$ en ∞ de una función $f(x)$ analítica en ∞ se define como el cociente P/Q con P y $Q \neq 0$ polinomios de grado a lo sumo n verificando:*

$$f(x) - \frac{P(x)}{Q(x)} = \mathcal{O}\left(x^{-2n-1}\right).$$

Al tomar una función específica se llega a la familia buscada:

Teorema 3.17 *Sea P/Q la aproximante de Padé de orden $[2N/2N]$ en ∞ de la función:*

$$f(x) = \frac{1}{2} + \frac{1}{2}\sqrt{\frac{(x+1)(x-2)}{x(x-1)}},$$

normalizada de forma que $2^{-N}Q$ es mónico. Entonces P/Q viene dada por P_N/Q_N correspondiente al paso N-ésimo de las ecuaciones de recurrencia:

$$\begin{cases} P_0(k) = Q_0(k) = 1, \\ P_{N+1}(k) = (2k^2 - 2k - 1)P_N(k) - Q_N(k), \\ Q_{N+1}(k) = 2k(k-1)P_N(k) - Q_N(k); \end{cases}$$

y las expresiones:

$$x_N(k) = kP_N(k) - Q_N(k), \qquad y_N(k) = (1-k)P_N(k) + kQ_N(k)$$

dan una solución polinómica de $(K4)$ con x_N, $y_N \in \mathbb{Z}[k]$ y $\deg(x_N) = 1 + \deg(y_N) = 2N + 1$.

Demostración. Colocando en (P) $u = 2x - 1$, $v = 1$, se tiene la ecuación de Pell generalizada:

$$a(x)\mu^2 - b(x)\lambda^2 = 1, \qquad a(x) = \frac{1}{2}x(x-1), \quad b(x) = \frac{1}{2}(x+1)(x-2).$$

Para todo $k \in \mathbb{Z}$, se cumple que $a(k)$, $b(k) \in \mathbb{Z}$, ya que siempre al menos uno de los factores de $a(x)$ y $b(x)$ es par. Dado que $a(x) - b(x) = 1$, se tiene la solución minimal obvia $\lambda = \mu = 1$ y los polinomios λ_N, $\mu_N \in \mathbb{Q}[x]$ definidos por:

$$\mu_N(x)\sqrt{a(x)} + \lambda_N(x)\sqrt{b(x)} = \left(\sqrt{a(x)} + \sqrt{b(x)}\right)^{2N-1}, \qquad N \in \mathbb{Z}^+$$

resuelven la ecuación. Además, para todo $k \in \mathbb{Z}$, se cumple que $\mu_N(k)$, $\lambda_N(k) \in \mathbb{Z}$. En otras palabras, se tienen sucesiones respectivas $\{\mu_N\}_{N=1}^{\infty}$, $\{\lambda_N\}_{N=1}^{\infty}$ en $\mathbb{Q}[x]$ con $\mu_0(x) = \lambda_0(x) = 1$ verificando la ecuación de recurrencia:

$$\begin{aligned} \mu_{N+1}(x)\sqrt{a(x)} + \lambda_{N+1}(x)\sqrt{b(x)} &= \left(\mu_N(x)\sqrt{a(x)} + \lambda_N(x)\sqrt{b(x)}\right)\left(\sqrt{a(x)} + \sqrt{b(x)}\right)^2 \\ &= \left[\mu_N(x)\left(a(x) + b(x)\right) + 2\lambda_N(x)b(x)\right]\sqrt{a(x)} + \left[2a(x)\mu_N(x) + \lambda_N(x)\left(a(x) + b(x)\right)\right]\sqrt{b(x)}, \end{aligned}$$

o de forma equivalente:

$$\begin{cases} \mu_0(x) = \lambda_0(x) = 1, \\ \mu_{N+1}(x) = (x^2 - x - 1)\mu_N(x) + (x+1)(x-2)\lambda_N(x), \\ \lambda_{N+1}(x) = x(x-1)\mu_N(x) + (x^2 - x - 1)\lambda_N(x). \end{cases}$$

Por inducción, μ_N, $\lambda_N \in \mathbb{Z}[x]$ y denotando por $\mathrm{lc}(\mu_N)$, $\mathrm{lc}(\lambda_N)$ a sus coeficientes principales, estos y los grados de cada uno corresponden a:

$$\mathrm{lc}(\mu_0) = \mathrm{lc}(\lambda_0) = 1 = 2^0, \qquad \mathrm{lc}(\mu_{N+1}) = \mathrm{lc}(\lambda_{N+1}) = \mathrm{lc}(\mu_N) + \mathrm{lc}(\lambda_N) = 2 \cdot 2^N = 2^{N+1};$$

$$\deg(\mu_0) = \deg(\lambda_0) = 0 = 2 \cdot 0, \qquad \deg(\mu_{N+1}) = \deg(\lambda_{N+1}) = \deg(\mu_N) + 2 = \deg(\lambda_N) + 2 = 2N + 2 = 2(N+1).$$

Además, también por inducción todos los coeficientes de $\mu_N(x)+\lambda_N(x)$ son pares, ya que:

$$\mu_0(x)+\lambda_0(x)=2, \qquad \mu_{N+1}(x)+\lambda_{N+1}(x)=(2x^2-2x)\left(\mu_N(x)+\lambda_N(x)\right)-\left(\mu_N(x)+\lambda_N(x)\right)-2\lambda_N(x).$$

Por otra parte, la ecuación de Pell generalizada del principio verifica al dividirla entre $a(x)\lambda_N^2(x)$:

$$\left(\frac{\mu_N(x)}{\lambda_N(x)}-(2f(x)-1)\right)\left(\frac{\mu_N(x)}{\lambda_N(x)}+(2f(x)-1)\right)=\frac{1}{a(x)\lambda_N^2(x)},$$

por lo que para x grande:

$$\left|\frac{\mu_N(x)}{\lambda_N(x)}-(2f(x)-1)\right|\leq\frac{1}{\lambda_N(x)\sqrt{a(x)}}\ll\frac{1}{x^{\deg(\lambda_N)}\sqrt{x(x-1)}}\ll x^{-2N-1}.$$

Esto quiere decir que $\mu_N(x)/\lambda_N(x)$ es la aproximante de Padé de orden $[2N/2N]$ en ∞ de $2f(x)-1$ y los polinomios correspondientes a la misma son $P=(\mu_N+\lambda_N)/2$ y $Q=\lambda_N$. Más aún, puesto que despejando se tiene $\mu_N=2P-Q$ y $\lambda_N=Q$, al sustituir las ecuaciones de recurrencia de μ_N y λ_N se obtiene una recurrencia para P y Q cuyas ecuaciones corresponden a las del enunciado. De esa manera, P/Q viene expresada de forma recurrente como P_N/Q_N y al sustituir $(\lambda,\mu,u,v)=(Q_N(k),2P_N(k)-Q_N(k),2k-1,1)$ con $k\in\mathbb{Z}$ en el Corolario 3.13 se concluyen las fórmulas para $x_N(k)$ e $y_N(k)$. Para finalizar, justamente la recurrencia de P_N y Q_N implica que $Q_N-P_N=P_{N-1}$. Por ello, $P_N(x)\sim Q_N(x)\sim 2^N x^{2N}$ y así, $x_N(k)\sim k y_N(k)\sim 2^N k^{2N+1}$. □

Es posible escribir los polinomios P_N y Q_N del Teorema 3.17 en términos de polinomios clásicos:

Corolario 3.18 *Para $k\in\mathbb{Z}_{>1}$ y $t:=k^2-k-1$, cada par:*

$$x_N(k)=(k-1)U_N(t)-U_{N-1}(t), \qquad y_N(k)=U_N(t)+kU_{N-1}(t);$$

donde U_N son los llamados polinomios de Chebyshev de segunda especie, proporciona una solución no trivial de $(K4)$.

Demostración. De las ecuaciones de recurrencia para P_N y Q_N se obtiene:

$$Q_{N+1}(k)=P_N(k)+P_{N+1}(k), \qquad P_{N+2}=(2k^2-2k-1)P_{N+1}(k)-Q_{N+1}(k)=2tP_{N+1}(k)-P_N(k),$$

con $P_0(k)=1$, $P_1(k)=2t$. La recurrencia sobre P_{N+2} no es más que la recurrencia que define a los polinomios de Chebyshev de segunda especie U_N, tomando $P_N(k)=U_N(k^2-k-1)=U_N(t)$. Como se cumple:

$$x_0(k)=kP_0(k)-Q_0(k)=k-1, \qquad x_1(k)=kP_1(k)-Q_1(k)=2(k-1)t-1=2k^3-4k^2+1,$$

$$\begin{aligned}x_{N+2}(k)+x_N(k)&=kP_{N+2}(k)-Q_{N+2}(k)+kP_N(k)-Q_N(k)\\&=2ktP_{N+1}(k)-(P_{N+2}(k)+P_{N+1}(k)+P_N(k)+P_{N-1}(k))\\&=2t\left(kP_{N+1}(k)-Q_{N+1}(k)\right)=2tx_{N+1}(k);\end{aligned}$$

$$y_0(k)=(1-k)P_0(k)+kQ_0(k)=1, \qquad y_1(k)=(1-k)P_1(k)+kQ_1(k)=2t+k=2k^2-k-2,$$

$$\begin{aligned}y_{N+2}(k)+y_N(k)&=(1-k)P_{N+2}(k)+kQ_{N+2}(k)+(1-k)P_N(k)+kQ_N(k)\\&=2(1-k)tP_{N+1}(k)+k(P_{N+2}(k)+P_{N+1}(k)+P_N(k)+P_{N-1}(k))\\&=2t\left((1-k)P_{N+1}(k)+kQ_{N+1}(k)\right)=2ty_{N+1}(k);\end{aligned}$$

tanto x_N como y_N satisfacen la misma recurrencia que U_N. Así, sustituyendo $P_N(k)=U_N(t)$, se concluyen las fórmulas para $x_N(k)$ e $y_N(k)$ en función de $U_N(t)$ del enunciado. □

Volviendo a aplicar las transformaciones de la Proposición 3.15, se puede generar de forma sucesiva una infinidad de familias polinómicas de soluciones. Sin embargo, es posible evitar la utilización de las aproximantes de Padé para construir una infinidad de familias polinómicas de soluciones si se aprovecha directamente la simetría $(\lambda,\mu)\leftrightarrow(u,v)$ existente en (P), tal y como muestra el siguiente resultado:

Proposicion 3.19 *Se consideran $\tau = 2k-1$ y los polinomios:*

$$A(\tau) = \frac{1}{2}\left(\tau^5+\tau^4-5\tau^3-5\tau^2+4\tau+2\right), \qquad B(\tau) = -\tau\left(\tau^4-5\tau^2+4\right), \qquad C(\tau) = \frac{1}{4}\tau\left(\tau^2-3\right)^2.$$

Sean los polinomios $P_M(k)$ y $Q_M(k)$ definidos por recurrencia como:

$$\begin{cases} P_0(k) = 2k-1, \quad Q_0(k) = k-1, \\ P_{M+1}(k) = A(\tau)P_M(k) + B(\tau)Q_M(k), \\ Q_{M+1}(k) = C(\tau)P_N(k) + (A(\tau)+B(\tau))Q_M(k). \end{cases}$$

Entonces, para cada $M \geq 0$:

$$x_M(k) = 2k(k-1)Q_M(k) - P_M(k), \qquad y_M(k) = (2k^2-2k-1)P_M(k) - (4k^2-4k-3)Q_M(k)$$

son polinomios en $\mathbb{Z}[k]$ verificando $(K4)$ para ciertos z_0, $z_1 \in \mathbb{Z}[k]$. Los coeficientes principales de x_M e y_M son positivos y $\deg(x_M) = 1+\deg(y_M) = 4M+3$.

Demostración. Se procede análogamente como en la prueba del Teorema 3.17 pero considerando que se resuelve una ecuación de Pell generalizada en términos de u y v en lugar de en λ y μ. Empezando de nuevo con $(\lambda,\mu,u,v) = (1,1,1-2k,1)$ se llega al problema de que $\lambda = \mu = 1$ produce en (P) la ecuación degenerada $v^2 - 0\cdot u^2 = 1$. Para resolver este problema, se considera una posibilidad más simple, y en este caso, la correspondiente a $(\lambda,\mu,u,v) = (2k^2-2k-1, 2k^2-2k-3, 1-2k, 1)$. Las dos primeras coordenadas corresponden a $\lambda_1(k)$ y $\mu_1(k)$ en el Teorema 3.17. La nueva ecuación de Pell generalizada asociada a (P) con esta elección de λ y μ sería:

$$c(k)v^2 - d(k)u^2 = 1, \qquad c(k) = 4k^4-8k^3+k^2+3k, \quad d(k) = k^2-k-1;$$

de la que de antemano se sabe que $(u_0(k), v_0(k)) = (\pm(2k-1), \pm 1)$ es solución. Tomando el signo + en $u_0(k)$ y $v_0(k)$ como solución mínima es posible generar nuevas soluciones a través de la recurrencia:

$$\begin{aligned} v_{M+1}(k)\sqrt{c(k)} + u_{M+1}(k)\sqrt{d(k)} &= \left(v_M(k)\sqrt{c(k)} + u_M(k)\sqrt{d(k)}\right)\left(\sqrt{c(k)} + \tau\sqrt{d(k)}\right)^2 \\ &= \left[2\tau d(k)u_M(k) + \left(\tau^2 d(k) + c(k)\right)v_M(k)\right]\sqrt{c(k)} + \left[\left(\tau^2 d(k)+c(k)\right)u_M(k) + 2\tau c(k)v_M(k)\right]\sqrt{d(k)}. \end{aligned}$$

Escribiendo los coeficientes en términos de $A(\tau)$, $B(\tau)$ y $C(\tau)$:

$$\tau^2 d(k) + c(k) = \frac{1}{2}\left(\tau^4-5\tau^2+2\right) = \frac{1}{2}\left(2A(\tau)+B(\tau)\right),$$

$$2\tau c(k) = \frac{1}{2}\tau\left(\tau^4-5\tau^2+4\right) = -\frac{1}{2}B(\tau), \qquad 2\tau d(k) = \frac{1}{2}\tau\left(\tau^2-5\right) = -\frac{1}{2}\left(B(\tau)+4C(\tau)\right);$$

se obtienen las ecuaciones de recurrencia:

$$\begin{cases} u_0(k) = \tau, \quad v_0(k) = 1, \\ u_{M+1}(k) = \frac{1}{2}(2A(\tau)+B(\tau))u_M(k) - \frac{1}{2}B(\tau)v_M(k), \\ v_{M+1}(k) = -\frac{1}{2}(B(\tau)+4C(\tau))u_M(k) + \frac{1}{2}(2A(\tau)+B(\tau))v_M(k). \end{cases}$$

Al efectuar el cambio $P_M(k) = u_M(k)$, $Q_M(k) = (u_M(k)-v_M(k))/2$, esta recurrencia se convierte en la del enunciado para $P_M(k)$ y $Q_M(k)$. Examinando los coeficientes, se cumple directamente que P_M, $Q_M \in \mathbb{Z}[k]$. Para la elección de λ y μ del principio, las fórmulas para $x_M(k)$ e $y_M(k)$ dadas tras aplicar el Corolario 3.13 son:

$$\begin{aligned} x_M(k) &= \frac{1}{4}\left((2k^2-2k-3)(u_M(k)+v_M(k)) + (2k^2-2k-1)(u_M(k)-3v_M(k))\right) \\ &= (k^2-k)(u_M(k)-v_M(k)) - u_M(k) = 2(k^2-k)Q_M(k) - P_M(k), \end{aligned}$$

$$\begin{aligned} y_M(k) &= \frac{1}{4}\left((2k^2-2k-3)(v_M(k)-u_M(k)) + (2k^2-2k-1)(u_M(k)+3v_M(k))\right) \\ &= (2k^2-2k-1)v_M(k) + \frac{u_M(k)-v_M(k)}{2} = (2k^2-2k-1)P_M(k) - (4k^2-4k-3)Q_M(k). \end{aligned}$$

A partir de la recurrencia para $u_M(k)$ y $v_M(k)$, por inducción se sigue que denotando por $\mathrm{lt}(u_M)$, $\mathrm{lt}(v_M)$ a sus términos principales, estos corresponden respectivamente a $2^{4M+1}k^{4M+1}$ y $2^{4M}k^{4M}$, ya que:

$$\mathrm{lt}(u_0) = 2k, \quad \mathrm{lt}(u_1) = \mathrm{lt}(\tau^5) = 2^5k^5,$$

$$\mathrm{lt}(u_{M+1}) = \mathrm{lt}\left(\tau^4\mathrm{lt}(u_M) + \tau^5\mathrm{lt}(v_M)\right) = \mathrm{lt}\left(\tau^4 \cdot \tau^{4M+1} + \tau^5 \cdot \tau^{4M}\right) = 2^{4(M+1)+1}k^{4(M+1)+1},$$

$$\mathrm{lt}(v_0) = 1, \quad \mathrm{lt}(u_1) = \mathrm{lt}(\tau^4) = 2^4k^4,$$

$$\mathrm{lt}(v_{M+1}) = \mathrm{lt}\left(\tau^3\mathrm{lt}(u_M) + \tau^4\mathrm{lt}(v_M)\right) = \mathrm{lt}\left(\tau^3 \cdot \tau^{4M+1} + \tau^4 \cdot \tau^{4M}\right) = 2^{4(M+1)}k^{4(M+1)}.$$

De esta manera, los términos principales de $x_M(k)$ e $y_M(k)$ son $\mathrm{lt}(x_M) = k^2\mathrm{lt}(u_M) = 2^{4M+1}k^{4M+3}$ y $\mathrm{lt}(y_M) = 2k^2\mathrm{lt}(v_M) = 2^{4M+1}k^{4M+2}$. □

E. Ecuaciones de Pell polinómicas y puntos de torsión. Toda solución de la ecuación de Pell generalizada $AX^2 - BY^2 = 1$ da lugar a una solución de la ecuación de Pell clásica $X^2 - ABY^2 = 1$, ya que:

$$1 = \left(X\sqrt{A} + Y\sqrt{B}\right)^2\left(X\sqrt{A} - Y\sqrt{B}\right)^2 = \left(AX^2 + BY^2 + 2XY\sqrt{AB}\right)\left(AX^2 + BY^2 - 2XY\sqrt{AB}\right)$$

y así basta realizar el cambio $X \mapsto AX^2 + BY^2$, $Y \mapsto 2XY$. Por tanto, cualquier solución polinómica de $(K4)$ produce una solución de la *ecuación de Pell polinómica* $X^2(x) - D(x)Y^2(x) = 1$. La existencia de soluciones no triviales para este tipo de ecuación de Pell en general no es clara[6] y el encontrar condiciones sobre D que permitan tal existencia es un problema abierto como se muestra en [**?**], [**?**], [**?**], [**?**], [**?**], [**?**], [**?**]. El caso más relevante aquí es aquél en que $\deg(D) = 4$, ya que la curva asociada $y^2 = D(x)$ satisface el siguiente resultado de Avanzi-Zannier [**?**]:

Teorema 3.20 *La ecuación $X^2 - D(x)Y^2 = 1$ con $D(x)$ polinomio cuártico mónico y libre de cuadrados tiene solución no trivial si y solo si la diferencia de los puntos del infinito de la curva elíptica $y^2 = D(x)$ es un punto de torsión de la misma.*

Sea la ecuación de Pell polinómica construida a partir de (P):

$$\Lambda^2 - D(u,v)M^2 = 1 \qquad D(u,v) = \frac{(9v^2 - u^2)(v^2 - u^2)}{64}.$$

Para que la ecuación $y^2 = D(u,v)$ cumpla $\deg(D) = 4$, u y v deben ser a lo sumo polinomios lineales, es decir $u = u_1x + u_2$, $v = v_1x + v_2$, de tal forma que $D(x)$ sea, tras algún cambio necesario, mónico y libre de cuadrados. Una vez se tenga eso, se puede aplicar el Teorema 3.20 para discernir si existen soluciones polinómicas de (P) con u y v polinomios lineales aparte del par $(2k-1, 1)$ que ya se conoce y se ha estudiado en el apartado anterior. Una primera observación al respecto es que no es necesario estudiar toda esta generalidad, ya que con los cambios adecuados se pueden simplificar los casos que hay que contemplar. Si el objetivo es buscar polinomios Λ, $M \in \mathbb{Q}[x]$ que satisfagan $\Lambda(x)^2 - D(u_1x + u_2, v_1x + v_2)M(x)^2 = 1$, dada la simetría existente entre u y v salvo constantes, es posible establecer una casuística respecto de u o respecto de v. Por ejemplo, si v no es constante, con la sustitución $x = (x' - v_2)/v_1$, el objetivo perseguido es equivalente a encontrar polinomios Λ', $M' \in \mathbb{Q}[x']$ tales que $\Lambda'(x)^2 - D(u_1'x + u_2', x')M'(x)^2 = 1$ para ciertos u_1' y u_2. Por otra parte, si v fuera constante ($v_1 = 0$ y $v_2 \neq 0$), la sustitución $v = v_2$ hace que el objetivo sea equivalente a que $\Lambda(x)^2 - D((u_1x + u_2)/v_2, 1)(v_2M(x))^2 = 1$. En resumen, basta estudiar sin pérdida de generalidad los caso en que $v = x$ y $v = 1$, obteniendo las curvas asociadas siguientes:

$$(x, 1) \quad \Rightarrow \quad e_1 : y^2 = D(x) = \frac{1}{64}(x^2 - 1)(x^2 - 9),$$

$$(mx + n, x) \quad \Rightarrow \quad e_2 : y^2 = D(x) = \frac{1}{64}((m^2 - 9)x^2 + 2mnx + n^2)((m^2 - 1)x^2 + 2mnx + n^2).$$

Una vez hecho esto, solo queda exigir que $D(x)$ sea mónico.[7] Posteriormente, la estrategia para calcular los puntos del infinito será pasarlos a la parte afín a través del cambio:

$$x \mapsto \alpha + \frac{\beta}{X}, \qquad y \mapsto \gamma\frac{Y}{X^2}$$

[6] A priori, puede decirse que $D(x)$ debe tener grado par, ya que en caso contrario en la expresión $X^2 - D(x)Y^2$ siempre aparecería algún término de grado impar que no puede ser cancelado y por tanto, la expresión jamás podría ser 1.

[7] Si $D(x)$ no es mónico, los puntos del infinito que se calculen posteriormente no tendrán coordenadas racionales, salvo que el coeficiente principal sea un cuadrado, en cuyo caso se puede realizar un cambio sencillo para convertir $D(x)$ en mónico.

y de ahí evaluar $X = 0$. Tras esto, se calculará su diferencia y se comprobará si el resultado es un punto de torsión de la correspondiente curva.

En el caso de e_1, cuyo $D(x)$ es siempre libre de cuadrados, cambiando $y \mapsto y/8$, la curva elíptica e_1:

$$E_1 : y^2 = (x^2 - 1)(x^2 - 9).$$

A continuación, con el cambio $x \mapsto 1 - 4/X$, $y \mapsto 8Y/X^2$, se obtiene la curva transformada:

$$\mathbf{E_1} : Y^2 = (X - 2)(X + 2)(X - 1) = X^3 - X^2 - 4X + 4.$$

Uno de los aspectos más importantes de las curvas elípticas es la existencia de una forma de sumar puntos que la dota de una estructura de grupo aditivo. Como aspecto particular, sus *puntos de torsión* serán aquellos que sumados consigo mismos un cierto número de veces n den lugar al elemento neutro $\mathcal{O}$ del grupo (que en la *forma de Weierstrass* $Y^2 = X^3 + AX + B$ de la curva corresponderá a ∞). Aplicando esto a $\mathbf{E_1}$, al sustituir $X = 0$ y despejar Y se obtienen los puntos del infinito $P_\pm = (0, \pm 2) \in \mathbb{Q}^2$. Puesto que los puntos son inversos, se cumple la relación $P_+ - P_- = 2P_+$. En general, para calcular $2P = 2 \cdot (X, Y)$ se toma la recta tangente a la curva en el punto P, que es de la forma $Y = Y'(0)(X - 0) + Y(0)$, se interseca con la curva y se comprueba el tercer punto de corte. Para ver que el tercer punto es de torsión, una forma de hacerlo es ver si el punto corresponde a un factor de la curva, ya que al ser $Y = 0$ entonces la tangente a la curva en P sería vertical, o lo que es lo mismo, $2P = \infty$. Aplicado a $\mathbf{E_1}$, la ecuación de la recta tangente en P_+ es $Y = -X + 2$. Al sustituir en la curva, se obtiene $(X - 2)\left(X^2 + X - 2\right) = (X - 2)^2$. De aquí hay dos opciones, o $X = 2$ o (simplificando el factor común) $X^2 = 0$, por lo que se consiguen los puntos $(2, 0)$ y $(0, 2)$ doble. Por tanto, $P_+ - P_- = (2, 0)$, que es un punto de torsión de orden 2 ya que $X - 2$ es un factor del segundo miembro de $\mathbf{E_1}$.

En el caso de e_2, dado que el coeficiente de x^4 es variable, únicamente se podrán estudiar aquellos valores de m que hagan de dicho coeficiente un cuadrado y aquellos valores de m y n tales que $D(x)$ sea libre de cuadrados para poder aplicar el Teorema 3.20. Factorizando $D(x)$, la única posibilidad de que no sea libre de cuadrados es que $n = 0$. Quitando este caso, $D(x)$ siempre será libre de cuadrados. El estudio se reduce, pues, a comprobar qué valores de m hacen al coeficiente principal de $D(x)$ un cuadrado, es decir, el estudio se reduce al de los puntos racionales de E_1. Para calcular los puntos racionales de $\mathbf{E_1}$, se puede escribir en `sagemath` el siguiente código:

```
E = EllipticCurve([0,-1,0,-4,4])
print E.rank()
print E.torsion_points()
```

La salida de este código muestra que el *rango*[8] de $\mathbf{E_1}$ es 0, por lo que hay un número finito de puntos racionales que corresponden a los elementos del subgrupo de torsión, formado por los puntos proyectivos:

$$\{(-2 : 0 : 1), (0 : -2 : 1), (2 : 0 : 1), (0 : 2 : 1), (4 : -6 : 1), (4 : 6 : 1), (1 : 0 : 1), (0 : 1 : 0)\}.$$

Por tanto, deshaciendo el cambio para volver a E_1 se concluye que:

$$E_1(\mathbb{Q}) = \{(-3, 0), (-1, 0), (1, 0), (3, 0), (0, -3), (0, 3), \infty\}.$$

Haciendo corresponder estos puntos con los valores $m = \pm 1, \pm 3$ que anulan el coeficiente de x^4, estos hacen que $D(x)$ tenga grado impar, por lo que no producen soluciones de $\Lambda^2 - D(x)M^2 = 1$. Por último, con $(0, -3)$ y $(0, 3)$ se tiene $m = 0$ y en ese caso $(u, v) = (mx + n, x) = (n, x)$, que se puede reducir al par $(x, 1)$ siempre que $n \neq 0$, que es un caso ya estudiado.

Con esto puede conluirse que en los casos en los que se ha podido aplicar el Teorema 3.20, la única familia polinómica se reduce esencialmente a $(x, 1)$ o bien $(1, x)$, y como u como v eran impares, solo se obtienen las familias lineales que ya se conocían $(2k - 1, 1)$ y $(1, 2k - 1)$. Lo que ocurra fuera de las condiciones del Teorema 3.20 sigue siendo desconocido.

§3. El caso $\mathcal{S}_5$

Antes de entrar en materia, esta última Sección hace uso de nociones básicas de *Geometría Algebraica* que deben tenerse en cuenta para poder entender todo su contenido, dejando detalles más complejos o que se salen de

[8] Véase Sección 3.

la intención de esta Sección para las referencias bibliográficas.

A modo de introducción, una curva algebraica C definida sobre $\mathbb{Q}$ (en general sobre $\mathbb{C}$) tiene asociada una importante característica topológica $g \in \mathbb{Z}_{\geq 0}$ llamada *género*. El género indica que la llamada *característica de Euler* de C considerada como *superficie de Riemann*[9] es $2-2g$. Para cada valor de g, el número obtenido muestra una equivalencia topológica (y por tanto una clasificación) entre C y un objeto de propiedades más conocidas, como las esferas o los toros de n asas. Cuando $g = 0$, la curva C se puede parametrizar [**?**] y si C cuenta con un punto racional, entonces tiene infinitos y la parametrización es racional. Cuando $g = 1$, la curva C será una *curva elíptica* [**?**], cuyo aspecto más interesante es, como se ha mencionado en la Sección anterior, su estructura de grupo aditivo asociada. De esta forma, si C cuenta con un punto racional P, entonces sumando P consigo mismo sucesivamente se irán obteniendo infinitos puntos racionales, a no ser que P sea de torsión. Los puntos de torsión son sencillos de identificar, pero no ocurre lo mismo con los que no lo son. En este sentido, la teoría de curvas elípticas da información sobre su estructura como suma directa de la parte de torsión y una parte libre $\mathbb{Z}^r$ con r un entero no negativo llamado *rango* (*Teorema de Mordell-Weil*). Por último, cuando $g > 1$, el celebrado *Teorema de Faltings* [**?**] afirma que el número de puntos racionales existentes en C es finito. Esto permitió ser aplicado en contextos tan fuertes como el *Último Teorema de Fermat*, anteriormente a la prueba de Wiles. La curva $x^n + y^n = 1$ tiene género $g = (n-1)(n-2)/2$. Si $n = 1$, entonces $g = 0$ y hay infinitas soluciones racionales. Si $n = 3$, entonces $g = 1$ y la curva define una curva elíptica que podría tener infinitos puntos racionales, aunque Euler probó que solo contiene los puntos de torsión $(1, 0)$ y $(0, 1)$. Finalmente, para cada $n > 3$ la deducción más fuerte es que solo habría un número finito de soluciones según el *Teorema de Faltings*. Por tanto, para $x = X/Z$, $y = Y/Z$; con X, Y y Z coprimos, la ecuación de Fermat $X^n + Y^n = Z^n$ tiene infinitas soluciones para $n = 2$ (ternas pitagóricas), las triviales para $n = 3$ y un número finito de soluciones no triviales para cada $n > 3$, si bien Wiles probó posteriormente que en realidad no hay ninguna en este último caso.

Cuando el número de variables aumenta las cosas se vuelven mucho más complejas y oscuras. Aunque el hecho de que el número de variables sea grande, haya soluciones reales y no haya problemas al tomar congruencias indica que la existencia de soluciones racionales podría ser mucho más plausible, esto no siempre es así. En el caso de las superficies algebraicas, para empezar, no es fácil establecer una clasificación. En esta dirección, existen conceptos más allá del *género* que da lugar a la conocida como *Clasificación de Enriques-Kodaira* [**?**], que deja entrever la existencia de diez tipos de situaciones diferentes que pueden ocurrir en las superficies algebraicas desde el punto de vista de la *Geometría Algebraica*. Uno de estos tipos lo conforman las denominadas *superficies de tipo general* (más o menos aquellas que no tienen particularidades especiales). Fuera de este grupo se encuentran tipos como las *superficies racionales* (las que se parametrizan mediante funciones racionales) y las *superficies K3*. Para ilustrar la enorme dificultad que entrañan este tipo de situaciones, Euler conjeturó que la superficie K3 $x^4 + y^4 + z^4 = 1$ no tiene puntos racionales no triviales pero más de dos siglos después se encontró [**?**] no solo un contraejemplo sino una infinidad de ellos y además distribuidos por doquier. Esta tarea no resultó nada fácil ni siquiera a través de una máquina, lo cual resulta algo sorprendente y da idea de la poca fiabilidad que en ocasiones la evidencia numérica revela. Todo ello obviamente sin decir nada de la extraordinaria dificultad teórica que subyace detrás de semejantes enunciados.

Sobrevolando todo el contexto anterior, en esta última Sección se presenta un resultado parcial acerca del conjunto $\mathcal{S}_5$, protagonista de la Conjetura 3.1. La evidencia numérica parece apoyar dicha conjetura, lo cual se refleja incluso tomando familias polinómicas de la Sección anterior. Como ejemplo de ello, al tomar la familia de soluciones de $(K4)$ dada por $x(k) = 2k^3 - 4k^2 + 1$, $y(k) = 2k^2 - k - 2$; y sustituirla en la tercera ecuación de $(K5)$ se obtiene una curva de género 2 dada por:

$$z_2^2 = 4k^6 + 8k^5 - 40k^4 + 45k^2 - 2k + 1.$$

Usando el llamado *Método de Chabauty* [**?**], el profesor X. Xarles probó que no existen puntos de coordenadas enteras sobre esa curva. En consecuencia, para todo $k \in \mathbb{Z}^+$, el $n = (x^2-1)(y^2-1)/4$ asociado no está en $\mathcal{S}_5$. Para descubrir el tipo de superficie algebraica que describen las ecuaciones de $(K5)$ es posible emplear `magma`. Para establecer una relación entre puntos racionales y puntos enteros en la superficie algebraica resulta conveniente homogeneizar previamente las ecuaciones considerándolas dentro de un espacio proyectivo:

$$X^2 + Y^2 - w^2 - Z_0^2, \qquad X^2 + 4XY + Y^2 + 3w^2 - Z_1^2, \qquad X^2 + 6XY + Y^2 + 8w^2 - Z_2^2.$$

[9] Al introducir una parametrización en C a través de números complejos, C puede interpretarse como superficie (*superficie de Riemann*). Por otra parte, algunos espacios topológicos poseen un invariante llamado *característica de Euler* y en el caso de las curvas algebraicas, se asocia a su superficie de Riemann correspondiente. Este invariante permite establecer criterios de clásificación de espacios topológicos, un tema central de la *Topología Algebraica*.

De esta forma, para ver su tipo según la *Clasificación de Enriques-Kodaira*, es posible utilizar el siguiente código:

```
P<x,y,z0,z1,z2,w> = ProjectiveSpace(Rationals(),5);
X = Surface(P,[x^2 + y^2 - w^2 - z0^2, x^2 + 4*x*y + y^2 + 3*w^2 - z1^2,
        x^2 + 6*x*y + y^2 + 8*w^2 - z2^2]);
KodairaEnriquesType(X);
```

La salida del código es `0 -2 K3` . Ignorando los dos valores numéricos, el tercer valor que aparece como texto es el tipo de la superficie algebraica. Por tanto, el objeto algebraico definido por $(K5)$ es una superficie K3 y el ejemplo de $x^4 + y^4 + z^4 = 1$ hace desconfiar como se ha comentado de la evidencia numérica. El problema de este tipo de superficies está en que no hay una conjetura clara acerca de los puntos racionales y en este caso además habría que pasar a puntos enteros.

Una forma de atajar, aunque no solucionar totalmente, este problema es asociar a $(K5)$ una superficie de tipo general de modo que la llamada *Conjetura de Bombieri-Lang* [**?**] arroje algún resultado. Esta conjetura sostiene en el caso de superficies sobre $\mathbb{Q}$ que en una superficie algebraica suave de tipo general el conjunto de puntos racionales no es Zariski denso, es decir, que los posibles puntos racionales deben estar contenidos en un cierto número de curvas dentro de la superficie. Si las curvas tienen género 0 o 1, puede haber infinitos puntos pero la gran ventaja es que los mismos estarían localizados, no distribuidos arbitrariamente como en el caso de $x^4+y^4+z^4 = 1$ descrito anteriormente.

Además de tener presente la *Conjetura de Bombieri-Lang*, se asumirá otra condición extra:

Conjetura 3.21 *No existen funciones racionales $x(t)$, $y(t)$, $z_j(t) \in \mathbb{Q}(t)\backslash\mathbb{Q}$ verificando $(K5)$.*

Con las dos conjeturas asumidas, es posible llegar al siguiente resultado parcial:

Teorema 3.22 *Bajo la Conjetura de Bombieri-Lang y la Conjetura 3.21, el conjunto $\mathcal{S}_5$ es finito.*

Demostración. Por el Corolario 3.13 toda solución de $(K4)$ procede de una solución de (P). Imponiendo la condición extra de $(K5)$, a través de las fórmulas de x e y dadas en el mismo Corolario se obtienen las siguientes ecuaciones:

$$\begin{cases} -\lambda^2u^2 + \mu^2u^2 + 9\lambda^2v^2 - \mu^2v^2 - 8 = 0, \\ 2\lambda^2u^2 - \mu^2u^2 + 10\lambda\mu uv - 9\lambda^2v^2 + 2\mu^2v^2 + 32 = 4z_2^2. \end{cases}$$

Estas ecuaciones definen una variedad afín de dimensión 3 (número de variables independientes). Sin embargo, es posible reducir su dimensión con el siguiente cambio de variables:

$$X = \frac{\lambda}{\mu}, \qquad Y = \frac{u}{v}, \qquad Z = \mu v, \qquad Z_2 = \frac{z_2}{\mu v};$$

el cual lleva a una superficie algebraica (variedad algebraica de dimensión 2) en $\mathbb{A}^4$:

$$\begin{cases} Z^2(-X^2Y^2 + Y^2 + 9X^2 - 1) = 8, \\ -2X^2Y^2 + 3Y^2 + 10XY + 27X^2 - 2 = 4Z_2^2, \end{cases}$$

Es importante notar que cada solución entera no trivial de $(K5)$ produce una tupla (X, Y, Z, Z_2) con X, Y, $Z_2 \in \mathbb{Q}$ y $Z \in \mathbb{Z}$. Si se homogeneizan las ecuaciones, la variedad V resultante de $\mathbb{P}^4$ no es irreducible, ya que al comprobar el tipo de V en `magma` [**?**] a través del código:

```
P<x,y,z0,z1,z2,w> = ProjectiveSpace(Rationals(),5);
V = Surface(P,[z^2 * (- x^2*y^2 + y^2*w^2 + 9*x^2*w^2 - w^4) - 8*w^6,
        - 2*x^2*y^2 + 3*y^2*w^2 + 10*x*y*w^2 + 27*x^2*w^2 - 2*w^4 - 4*z2^2*w^2]);
KodairaEnriquesType(V);
```

se produce el error `Runtime error in 'Surface': Scheme is not reduced and irreducible` . El problema está en que V contiene varias superficies (factores irreducibles) en realidad. Por ello, hay que identificarlas y extraer las que sean importantes. Es posible extraer estos factores irreducibles escribiendo el siguiente código en `sagemath` [**?**]:

```
P<x,y,z,z2,w> = ProjectiveSpace(4,QQ)
P1 = z^2*(-x^2*y^2+y^2*w^2+9*x^2*w^2-w^4)-8*w^6
P2 = -2*x^2*y^2+3*y^2*w^2+10*x*y*w^2+27*x^2*w^2-2*w^4-4*z2^2*w^2
V = P.subscheme([P1,P2])
print V.irreducible_components()
```

La salida del código muestra que V contiene tres trozos, correspondientes a los hiperplanos proyectivos $\{Y = w = 0\}$ y $\{X = w = 0\}$, y al ideal generado por los cuatro polinomios siguientes:

$$\begin{cases} P_1 := & 9X^2Z^2 + 10XYZ^2 + Y^2Z^2 - 4Z^2Z_2^2 + 16w^4, \\ P_2 := & 2X^2Y^2 - 27X^2w^2 - 10XYw^2 - 3Y^2w^2 + 4Z_2^2w^2 + 2w^4, \\ P_3 := & 10XY^3Z^2 + Y^4Z^2 - 4Y^2Z^2Z_2^2 - 90XYZ^2w^2 + 36Z^2Z_2^2w^2 + 16Y^2w^4 - 9Z^2w^4 - 216w^6, \\ P_4 := & Y^5Z^2 + 40XY^2Z^2Z_2^2 - 4Y^3Z^2Z_2^2 - 90XY^2Z^2w^2 - 100Y^3Z^2w^2 - 360XZ^2Z_2^2w^2 + 36YZ^2Z_2^2w^2 \\ & -160XY^2w^4 + 16Y^3w^4 + 90XZ^2w^4 + 91YZ^2w^4 + 2160Xw^6 + 584Yw^6. \end{cases}$$

Utilizando ahora `magma` se puede confirmar que $P_1 = P_2 = P_3 = P_4 = 0$ define una superficie S se tipo general en $\mathbb{P}^4$ escribiendo el siguiente código:

```
P<x,y,z,z2,w> := ProjectiveSpace(Rationals(),4);
P1 := 9*x^2*z^2 + 10*x*y*z^2 + y^2*z^2 - 4*z^2*z2^2 + 16*w^4;
P2 := 2*x^2*y^2 - 27*x^2*w^2 - 10*x*y*w^2 - 3*y^2*w^2 + 4*z2^2*w^2 + 2*w^4;
P3 := 10*x*y^3*z^2 + y^4*z^2 - 4*y^2*z^2*z2^2 - 90*x*y*z^2*w^2 + 36*z^2*z2^2*w^2
        + 16*y^2*w^4 - 9*z^2*w^4 - 216*w^6;
P4 := y^5*z^2 + 40*x*y^2*z^2*z2^2 - 4*y^3*z^2*z2^2 - 90*x*y^2*z^2*w^2 - 100*y^3*z^2*w^2
        - 360*x*z^2*z2^2*w^2 + 36*y*z^2*z2^2*w^2 - 160*x*y^2*w^4 + 16*y^3*w^4 + 90*x*z^2*w^4
        + 91*y*z^2*w^4 + 2160*x*w^6 + 584*y*w^6;
X := Surface(P,[P1, P2, P3, P4]);
KodairaEnriquesType(X);
```

La salida ahora es `2 0 General type` , que es lo que se buscaba. Con esto, gracias al Corolario 3.13, que impone condiciones algebraicas para tener soluciones enteras de $(K4)$, se ha podido transformar la superficie K3 definida por $(K5)$ en S. Por la *Conjetura de Bombieri-Lang* y el *Teorema de Faltings*, si existen puntos racionales en S, estos deben concentrarse en curvas de género 0 o 1. De entre ambos tipos, las de género 0 admiten una parametrización con funciones racionales y asumiendo la Conjetura 3.21 se evita la infinidad de puntos racionales que podría haber para producir soluciones no triviales. Faltaría probar que no hay una infinidad de puntos provenientes de soluciones de $(K5)$ en cualquier curva elíptica embebida en S. Para ello, se atiende al valor de Z. Por una parte, si Z es una constante fijada, la ecuación $Z^2(-X^2Y^2 + Y^2 + 9X^2 - 1) = 8$ define una curva birracionalmente equivalente a una curva elíptica. Para comprobarlo, el primer paso es cambiar $Y \mapsto Y/(1 - X^2)$:

$$Y^2Z^2(1 - X^2) + 9(1 - X^2)^2X^2Z^2 - (1 - X^2)^2Z^2 = 8(1 - X^2)^2.$$

Simplificando el factor $1 - X^2$, despejando Y^2Z^2 y aplicando como en otras ocasiones un cambio del tipo $X \mapsto \alpha + \beta/X$ se obtiene:

$$Y^2Z^2 = 8 - 8\alpha^2 - 8\frac{\beta^2}{X^2} - 16\frac{\alpha\beta}{X} + Z^2 - 10\alpha^2Z^2 - 10\frac{\beta^2}{X^2}Z^2 - 20\frac{\alpha\beta}{X}Z^2 + 9\left(\alpha^4 + 4\frac{\alpha^3\beta}{X} + 6\frac{\alpha^2\beta^2}{X^2} + 4\frac{\alpha\beta^3}{X^3} + \frac{\beta^4}{X^4}\right)Z^2.$$

Si $\alpha = 1$, varios términos pueden cancelarse entre sí, quedando:

$$Y^2Z^2 = -8\frac{\beta^2}{X^2} - 16\frac{\beta}{X} + \left(9\frac{\beta^4}{X^4} + 36\frac{\beta^3}{X^3} + 44\frac{\beta^2}{X^2} + 16\frac{\beta}{X}\right)Z^2.$$

Para quitar los denominadores se impone $Y \mapsto Y/X^2$:

$$Y^2Z^2 = 16\beta(1 - Z^2)X^3 + \left(44\beta^2Z^2 - 8\beta\right)X^2 + 36\beta^3Z^2X + 9\beta^4Z^2.$$

El siguiente paso es tomar $\beta = 2/(11Z^2)$ para eliminar el factor con X^2 y dividir toda la ecuación entre Z^2:

$$Y^2 = \frac{32(1 - Z^2)}{11Z^4}X^3 + \frac{288}{1331Z^6}X + \frac{144}{14641Z^8}.$$

Por último, se busca la forma de Weierstrass $Y^2 = X^3 + AX + B$ a través del cambio $Y \mapsto (32(1 - Z^2)/(11Z^4))^2Y$, $X \mapsto 32(1 - Z^2)X/(11Z^4)$, y simplificando se consigue la curva:

$$Y^2 = X^3 + \frac{9Z^6}{1024(1 - Z^2)^3}X + \frac{9Z^8}{65536(1 - Z^2)^4}.$$

El discriminante del segundo miembro es:

$$4A^3 + 27B^2 = -\frac{729}{4294967296} \cdot (13Z^2 + 3)Z^{16}(Z^2 - 1)^{-9}.$$

Por tanto, la ecuación de partida define una cuva elíptica para cada $Z \notin \{0, 1, -1\}$. Cuando se fija Z, examinando el cambio de variables del principio de la demostración se tiene que $(x, y) = (ZX, ZY)$ es un punto de coordenadas enteras en una curva elíptica fija y por el llamado *Teorema de Siegel* [**?**] existe únicamente un número finito de posibilidades. El caso $Z = 0$ lleva a contradicción ya que carece de sentido en la parte afín de S, mientras que si $Z = \pm 1$, la ecuación se convierte en $(X^2 - 1)(Y^2 - 9) = 0$. Por una parte, si $X^2 = 1$, el cambio de variables del principio implica que λ, $\mu \in \{-1, 1\}$ y gracias al Corolario 3.13 se concluye que x^2 o y^2 es 1, produciendo una solución trivial. Por otra parte, si $Y^2 = 9$, el cambio de variables del principio implica que $u \in \{3, -3\}$ y $v \in \{1, -1\}$ y gracias al Corolario 3.13 se concluye que x^2 o y^2 es 1, produciendo de nuevo una solución trivial. En resumen, se ha probado que es imposible encontrar infinitas soluciones no triviales de $(K5)$ que originen puntos sobre S con un Z fijado. Sea ahora el caso en que Z no es constante. Como se ha mencionado anteriormente, la *Conjetura de Bombieri-Lang* asegura que las soluciones racionales están sobre un conjunto finito de curvas de género 0 o 1. Considerando ahora que Z tiene un polo en el punto O se construyen a partir de este punto base y a través del *Teorema de Riemann-Roch* [**?**] funciones x e y con polos de orden 2 y 3 en O verificando la forma de Weierstrass $y^2 = x^3 + ax + b$ con a, $b \in \mathbb{Q}$ de una curva elíptica E. Con esta formulación, se puede probar la identidad:[10]

$$x^d + a_{d-1}(Z)x^{d-1} + \ldots + a_0(Z) = 0 \qquad \text{para algunos } a_j \in \mathbb{Q}[Z].$$

En efecto, si $\mathbb{Q}(E)$ es el *cuerpo de funciones* de E,[11] existe un polinomio $P \in \mathbb{Q}[x, y]$ con $y^2 = x^3 + ax + b$ tal que $ZP \in \mathbb{Q}[x, y]$ (basta tomar como $P(x)$ un polinomio que se anule con orden suficiente en los polos de Z diferentes de O). Como $y^2 \in \mathbb{Q}[x]$, es posible escribir $ZP(x) = B_0(x) + yB_1(x)$ con B_0, $B_1 \in \mathbb{Q}[x]$ de forma que:

$$(ZP(x) - B_0(x))^2 - B_1(x)^2(x^3 + ax + b) = 0.$$

Obviamente, los grados de B_0^2 y $x^3B_1^2$ son de diferente paridad. Entonces, si m es el orden del polo de ZP en O, se tiene:[12]

$$\deg(P^2) < m = \text{máx}\{2\deg(B_0), \deg(B_1^2x^3)\} = \deg(B_0^2 - B_1^2(x^3 + ax + b)).$$

Al desarrollar $(ZP(x) - B_0(x))^2 - B_1(x)^2(x^3 + ax + b) = 0$ y dividir por el coeficiente principal en x se obtiene la identidad buscada. Si se quitan ahora los denominadores de los coeficientes a_j, se deduce que para Z entero existe solamente un número finito de posibilidades para los denominadores de x e y.[13] De nuevo por el *Teorema de Siegel*,[14] existe solo un número finito de puntos racionales que originen valores enteros de Z. □

Como observación final, el resultado parcial que se ha obtenido da pie a un interrogante. ¿Es realmente necesaria la Conjetura 3.21 o puede rebajarse la condición? Hasta la fecha no se ha conseguido esclarecer si esta conjetura resulta tan fuerte como parece en vista de la demostración de este resultado. Queda como problema futuro el dilucidar algún resultado más fuerte según el cual el conjunto $\mathcal{S}_5$ sea finito o vacío.

[10] La prueba de esta identidad se sigue de [**?**] pero su justificación no resulta demasiado convincente. Por ello, la prueba presentada aquí busca solamente una explicación sencilla, sin reclamar originalidad.

[11] El *cuerpo de funciones* se define como el cuerpo de fracciones de $\mathbb{Q}[x, y]/I$, donde x e y son variables e I es el ideal generado por $x^3 + ax + b - y^2$.

[12] Cuando una función meromorfa $f(z)$ se comporta como $a/z^n + \ldots$ (términos de grado mayor) cerca del origen se dice que tiene en él un polo de orden n. Cambiando z por $1/z$ el origen pasa al infinito y se dice que $f(z)$ tiene un polo de orden n en el infinito si para n grande es como $az^n + \ldots$ (términos de grado menor). Con esta noción, el orden en un mismo punto de la composición de funciones de órdenes n_1 y n_2 es n_1n_2. En este caso, $P(x)$ tiene grado n y como está sustituido en x que tiene orden 2 en O (el infinito en términos de curvas elípticas) el orden del polo de $P(x)$ es $\deg(P^2) = 2\deg(P)$. Por otro lado, como Z tiene un polo en O, el orden del polo de ZP es mayor que $\deg(P^2)$ y de ahí la primera desigualdad.

[13] Un polinomio $a_0x^d + a_1x^{d-1} + \cdots \in \mathbb{Z}[x]$, si tiene una raíz racional, su denominador divide a a_0 (*Regla de Ruffini*). En particular, solo hay un número finito de posibilidades para x y por tanto también para y.

[14] El *Teorema de Siegel* se aplica no solo a puntos de coordenadas enteras como se ha visto previamente sino también a puntos de coordenadas racionales con denominador acotado.